

EXHIBIT 1

PUBLIC VERSION

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

NETWORK PROTECTION SCIENCES,
LLC

Plaintiff,

vs.

FORTINET, INC.

Defendants.

No. 3:12-CV-01106-WHA

REPLY EXPERT REPORT OF ANGELOS KEROMYTIS, PH.D.

Dated: July 24, 2013

Respectfully submitted,

By: Angelos D. Keromytis

Angelos Keromytis, Ph.D.

I. INTRODUCTION

1. I, Angelos Keromytis, submit this reply report on behalf of Network Protection Sciences, LLC. I submitted a report on infringement in this matter on July 3, 2013 and a report on validity on July 17, 2013 in relation to U.S. Patent No. 5,623,601 (“the ‘601 patent”). For this report, I have been asked to review and comment upon the July 17, 2013 Expert Report of Christian B. Hicks on non-infringement. For the reasons set forth in my opening report and discussed herein, I disagree with Mr. Hicks’s conclusion that Fortinet does not infringe claims 10, 19, 29, 43 or 57 of the ‘601 patent.

II. THE ACCUSED PRODUCTS

2. Mr. Hicks states that “[t]he firewalls created and sold by Fortinet are modern firewalls that are capable of and specifically designed for forwarding packets (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 337, NPS0056062 at NPS0056398). In particular, they commonly forward packets with NAT (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 183-184, 338-339 - NPS0056062 at NPS0056244-245, NPS0056399-400).” (Paragraph 6.3)

3. However, the citations Mr. Hicks provides do not support this proposition. First, Mr. Hicks cites to a portion of the FortiOS manual that recites:

Add a default route and gateway

A route provides the FortiGate unit with the information it needs to forward a packet to a particular destination. A static route causes packets to be forwarded to a destination other than the default gateway. You define static routes manually. Static routes control traffic exiting the FortiGate unit. You can specify through which interface the packet will leave and to which device the packet should be routed.

In the factory default configuration, entry number 1 in the Static Route list is associated with a destination address of 0.0.0.0/0.0.0.0, which means any/all

destinations. This route is called the “static default route”. If no other routes are present in the routing table and a packet needs to be forwarded beyond the FortiGate unit, the factory configured static default route causes the FortiGate unit to forward the packet to the default gateway. For an initial configuration, you must edit the factory configured static default route to specify a different default gateway for the FortiGate unit. This will enable the flow of data through the unit.

(Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 337, NPS0056062 at NPS0056398).

This passage simply indicates that a route needs to be defined so that the FortiGate can transmit an information packet away from the unit to a destination. Such a configuration does not demonstrate that the Accused Products operate in a manner that does not employ application layer proxies or employ IP forwarding as discussed in the ‘601 patent.

4. Second, Mr. Hicks cites to a portion of the FortiOS manual that recites:

Add firewall policies

Firewall policies enable traffic to flow through the FortiGate interfaces. Firewall policies define how the FortiGate unit processes the packets in a communication session. For the initial installation, a single firewall policy that enables all traffic to flow through will enable you to verify your configuration is working. On lower-end units such a default firewall policy is already in place. For the high-end FortiGate units, you need to add a firewall policy.

The following steps add two policies that allows all traffic through the FortiGate unit, to enable you to continue testing the configuration on the network.

These steps provide a quick way to get traffic flowing through the FortiGate unit. It is a very broad policy and not recommended to keep on the system once initial setup and testing are complete. You will want to add more restrictive firewall policies to provide better network protection.

(Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, 338-339 - NPS0056062 at NPS0056399-

400). As indicated in the manual, this policy cited by Mr. Hicks is simply used as a quick way to

get traffic flowing so that initial setup and testing can be done. However, users are instructed that this policy is “not recommended to keep on the systemYou will want to add more restrictive firewall policies to provide better network protection.” (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, 338-339 - NPS0056062 at NPS0056399-400). The extent of use of this policy is not significant because it does not provide UTM profiles and as Fortinet’s CTO Michael Xie testified, a majority of users employ UTM profiles. Similarly, at Paragraph 6.9, Mr. Hicks relies on a passage from the FortiOS manual on a default configuration for the FortiGate-100A. (FortiOS Handbook v. 3 for FortiOS 4.0 MR 2 p. 268, NPS0058504 at NPS0058771). However, this portion of the manual instructs a user to disable the default configuration “to simplify policy configuration and increase security. By deleting this policy you ensure that any traffic which does not match a configured policy is rejected...” (FortiOS Handbook v. 3 for FortiOS 4.0 MR 2 p. 268, NPS0058504 at NPS0058771).

5. Throughout his report Mr. Hicks relies on these and other passages from Fortinet’s materials to improperly conclude that the Accused Products engage in packet forwarding and assumes that these references to forwarding are the same as the IP forwarding that is discussed in the ‘601 patent. They are not. In the ‘601 patent the term forwarding is used in the context of a device that permits direct communication between the source and destination. (‘601 patent col. 6:14-36). This is referred to as IP forwarding. The Accused Products, by default as acknowledged by Mr. Hicks, do not incorporate this type of forwarding because they employ numerous operations for handling the packets between receipt and re-transmittal, including network address translation and transparent application layer proxies. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 189-200).

6. Fortinet’s materials use the term “forward” to describe a different concept, which is to

ultimately forward a data packet from the Accused Product to the destination after it has been processed by the Accused Product. As an example, the FortiOS manual states:

Example 1: client/server connection

The following example illustrates the flow of a packet of a client/web server connection with authentication and FortiGuard URL and antivirus filtering. This example includes the following steps:

Initiating connection from client to web server

- 1 Client sends packet to web server.
- 2 Packet intercepted by FortiGate unit interface.
 - 2.1 Link level CRC and packet size checking. If the size is correct, the packet continues, otherwise it is dropped.
- 3 DoS sensor - checks are done to ensure the sender is valid and not attempting a denial of service attack.
- 4 IP integrity header checking, verifying the IP header length, version and checksums.
- 5 Next hop route
- 6 Policy lookup
- 7 User authentication
- 8 Proxy inspection
 - 7.1 Web Filtering
 - 7.2 FortiGuard Web Filtering URL lookup
 - 7.3 Antivirus scanning
- 9 Source NAT
- 10 Routing
- 11 Interface transmission to network
- 12 Packet forwarded to web server

(Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 196).

As shown above, Fortinet's materials indicate that a data packet is "forwarded" to a destination after it is subject to the infringing application layer proxies. Just because Fortinet's materials state that a data packet is forwarded to a destination by a device does not mean that it is programmed to perform the same type of IP forwarding discussed in the '601 patent.

7. Moreover, Mr. Hicks improperly equates the use of NAT in the accused products to the IP forwarding discussed in the '601 patent. They are not the same and NAT prevents the direct

communication between the source and destination. As indicated in Fortinet's own materials, NAT is used by the Accused Products so that they are used as "a gateway between private and public networks." (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 183). With NAT "firewall policies perform the address translation between the internal and external interfaces." (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 184). An Accused Product looks "at the firewall policies to determine where the request should go [and] changes the packet information of the return address to its external interface, while keeping track of the originating user request, and the originating PC address." (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 184). When an Accused Product receives a response "it determines where it should go by looking at its session information [and] changes the destination IP to the correct user and delivers the packet." (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 185). As the preceding shows, when the Accused Product processes a packet using NAT, the packet is modified so that it appears to be coming from the Accused Product itself. The Accused Product will record the changes it makes in its state table. This illustrates that network address translation requires modifying a packet to prevent direct communication between a source and destination and does not involve IP forwarding as disclosed in the '601 patent. In fact, Fortinet's materials teach that NAT is a complementary process to the accused transparent application layer proxies, not an alternative to those proxies. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 193).

8. Mr. Hicks also states that "[w]hen forwarding with NAT, the packets are forwarded without creating any additional communications sessions, and without creating gateways between any communications sessions." (Paragraph 4.10). This conclusion is incorrect and inaccurate. NAT requires a stateful inspection of the communication packet so that it can perform persistent and consistent address mappings in both directions of communications. This

requires session information to be maintained at the firewall. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 185) (“it determines where it should go by looking at its session information [and] changes the destination IP to the correct user and delivers the packet.”)

9. In analyzing the Accused Products, Mr. Hicks also states that “[a] policy cannot, however, assign the process to the port number.” I disagree. As discussed in my opening report, the policy determines, based at least in part on a port number what proxy process is assigned to the port number. (FORT-NPS 017058-59; FORT-NPS 017008). As a result, the Accused Products assign a proxy processes based on port number, like the ‘601 patent. Further, Mr. Hicks’s analysis at paragraph 6.7 regarding the possibility of more than one policy or proxy process being assigned to a port number is irrelevant. The claims of the ‘601 patent do not preclude the possibility of more than one policy or proxy process from being assigned to a port number or used in connection with a gateway. For example, claim 19 of the ‘601 patent recites “at least one proxy process executable by the gateway station” and claim 43 recites “at least one proxy process that is configured to operate at an application layer of the gateway.”

10. At paragraph 6.8, Mr. Hicks indicates that Fortinet employs a “script to generate the default configurations” for the Accused Products. However, Mr. Hicks reliance on this information is flawed because, as discussed above, Fortinet instructs its users to disable this initial default setting and Fortinet’s CTO Michael Xie testified that a majority of users employ the accused application layer processes.

11. Mr. Hicks’s concludes that “as the Fortinet devices are configured when they are shipped, upon receipt of a packet, they would not create any additional communications sessions, and they would not create any gateways between any communications sessions.” (Paragraph 6.10). However, Mr. Hicks’s analysis fails to demonstrate that the accused products are not

programmed to include:

- “at least one proxy process executable by the gateway station, the at least one proxy process being adapted to transparently initiate a first communications session with a source of an initial data packet accepted by the operating system and to transparently initiate a second communications session with a destination of the packet without intervention by the source, and to transparently pass the data portion of packets received by the first communications session to the second communications session and to pass the data portion of packets received by the second communications session to the first communications session...”; or
- “means for establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;” or
- “means for transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions...”

12. Mr. Hicks also states that “even once configured by users, administrators would almost always configure their firewalls to allow outgoing connections to be forwarded with NAT. That means that outgoing packets would not be handled in a manner under which they would either be passed to an application layer process or else dropped. Instead, they would either be passed to an application layer process or else forwarded using NAT.” (Paragraph 6.11). However, these conclusions are not supported by evidence and testimony. As noted above, Fortinet’s CTO Michael Xie acknowledged that a majority of users employ application layer proxies. The

Accused Products have the same functionality for processing outbound traffic as inbound traffic. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, 192). Moreover, the Accused Products employ an outbound application layer process call Data Leak Prevention, which inspects the content of outbound traffic “to prevent sensitive data from leaving your network.” (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, 857). The configuration that Mr. Hicks claims is common would exclude this feature. An example showing that Mr. Hicks’s hypothesis is incorrect is demonstrated by the configuration files of Fortinet’s customer Qdoba, which shows that Qdoba’s Fortinet products were not only configured to enable UTM features such as Web Filtering, VoIP Inspection, Antivirus, and Email Filtering, but were also configured to perform Data Leak Prevention. (See Exhibit 1 and Qdoba.zip). Further, for the reasons discussed throughout this reply, this hypothesis is largely irrelevant because even if the Accused Products employ policies that allow outgoing connections using NAT: 1) the claims do not preclude gateways from employing other policies or processing in addition to application layer proxies and 2) the kernel is still modified to prevent forwarding of packets. While the Accused Products may or may not ship with a default policy that uses the NAT profile (which allows some traffic through), the system is built to never allow connections/traffic through unless a policy instructs it to.

13. Mr. Hicks further states that “[c]onfiguring policies so that no packets are forwarded on the Fortinet systems does not result in any changes to the Linux kernel on the system, nor does it result in any changes to the fortifilter module, or any other kernel module. The kernel on a Fortinet firewall is **always** capable of forwarding packets. Based on the rules set by the administrator, the system might decline to do so. But the kernel always remains capable of doing so.” (Paragraph 6.15). This conclusion is incorrect. As discussed in my opening report and

below, a policy is used to define the operations the Accused Products will perform on data packets, such as NAT or application layer proxies. Except for the operations identified by the policies, the kernel of the Accused Products is incapable of forwarding communications between two networks. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 232 (“If no policy matches, the connection is dropped”)). Thus, Mr. Hick’s claim that the “kernel on a Fortinet firewall is **always** capable of forwarding packets” is incorrect. The kernel requires the user to identify operations, such as NAT or application layer proxies which do not provide IP forwarding as disclosed in the ‘601 patent, through policies. Further, Mr. Hick’s assertion that policies do “not result in any changes to the Linux kernel on the system” is also incorrect. Fortinet’s 30(b)(6) witness, Mr. Crawford, testified that policies are in fact written in to the Linux kernel. Writing a policy to a kernel is still a modification of the kernel, since the policies are provided to, stored in, and enforced by the kernel. Mr. Hicks acknowledges as much in his report. (*See e.g.* Paragraph 6.3 quoting Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 231; Paragraph 6.14; FORT-NPS 164710-715).

14. Moreover, “modified” does not require “code changed.” A kernel can be modified to operate in a certain manner through configuration statements and does not need to have the code for the kernel rewritten to effect such a modification. Also, any skilled computer scientist who read the ‘601 patent and had any background in systems and security would understand that policies and code are interchangeable (and therefore constitute modifications); and would understand that permitting packet forwarding limits the degree of security provided by the firewall but does not materially alter the way the firewall operates with respect to transparent proxies.

III. CLAIMS 10 AND 43 OF THE '601 PATENT

15. Mr. Hicks states that there is “no evidence that the accused products have ever met the “else dropping the packet” limitations of claims 10 and 43.” (Paragraph 7.2.1) This is incorrect. As discussed in my opening report, the Accused Products require the use of a policy. The policy sets forth the processing that is employed to transmit a communication packet through the gateway. The policy assigns this processing based on, *inter alia*, port numbers. The policies also assign application layer proxies to these port numbers. Without a policy, the communication packet is dropped. This is a characteristic of and performed by all of the Accused Products. This characteristic is also confirmed by Fortinet’s user manuals and the testimony of Fortinet’s 30(b)(6) witness Mr. Crawford.

16. Mr. Hicks’s conclusions are also incorrect because Michael Xie testified that a majority of customers use the application layer processes provided by the Accused Products. So at the very least, as acknowledged by Michael Xie, a majority of users of the accused products employ a policy with an application layer proxy process assigned to at least one port.

17. Mr. Hicks’s conclusions are also incorrect as they apply to both claims in that he improperly assumes that the claims require an application layer proxy process bound to all ports. This is not the language of the claim and is not in accordance with the dependent claims. For instance, dependent claim 2 includes all of the requirements of claim 1 and recites:

2. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the step of determining involves checking to determine if a process is bound to the destination port number, and passing the packet to a generic process if a process is not bound to the destination port number, the generic process acting to establish the first and second communications sessions and to move the data between the first and second communications sessions.

18. As shown in dependent claim 2, the method of claim 1 may still be infringed if accused system assigns a process to some but not necessarily all of the destination port numbers. Similar requirements can be found in claim 11, which depends on claim 10.

19. For this reason, Mr. Hicks also incorrectly argues that “Claims 10 and 43 are not infringed if a customer is using packet forwarding with NAT for any of his outgoing connections, because for such a product, it is not true that “else the packet is dropped” is performed if it is not destined for a port that is assigned to a process on the firewall.” (Paragraph 7.2.3). Further, this statement is incorrect because the accused products’ network address translation feature involves processing used by the accused products that is not analogous to the IP forwarding feature discussed in the ‘601 patent.

20. Mr. Hicks also relies on the improper conclusion that “[a]n accused product cannot meet this claim element if it ever forwards a packet.” (Paragraph 5.3.4). Similarly, Mr. Hicks asserts that “[t]o infringe, an accused product must also drop all packets that are not destined for a port that is assigned to a process.” (Paragraph 5.3.5) Contrary to Mr. Hicks’s claim, an accused product can still meet this claim element if it forwards a packet before a determination is made on whether a proxy process is assigned to the corresponding port. For example, claim 10 says that there is a determining step on whether “there is a proxy process bound to a port for serving a destination port number of an accepted TCP/IP packet”, which precedes the setting up the first communications session, else dropping the packet. Similar language is present in claim 29 element (b) and claim 1 element (c). The “else dropping the packet” requires that a determination first be made, in the previous step. If there were selective processing of connections/packets (i.e. some packets/connections will be processed by proxies, while others will not), then the claim would still apply to the part that will be processed by the proxies in the

Accused Products.

21. With respect to the determining and establishing a first communication session steps of claims 10 and 43, Mr. Hicks asserts that these limitations are not present because “the accused products employ a system of policies that cannot and do not actually assign processes to ports.” (Paragraph 7.2.9). Mr. Hicks is incorrect. As discussed above, policies are necessary in order for the Accused Products to process the communications in any manner. The policies are used to configure the device and the operating system kernel. These policies assign the processes based in part on port number, including the transparent application layer processes.

22. Based on the opinions expressed in my opining report and as discussed above, contrary to Mr. Hicks’s conclusion, my analysis shows that the users of the Accused Products operate the devices in a manner that infringes claims 10 and 43 of the ‘601 patent.

23. At paragraph 7.2.5, Mr. Hicks improperly concludes that “The Keromytis Infringement Report lacks proper computer science evidence to show that any steps of claims 10 or 43 have been performed.” My analysis includes: inspecting the source code for the Accused Products, identifying routines that perform the infringing method steps, analyzing the manuals and user guides that describe the operation of the Accused Products, and reviewing engineer testimony about how the Accused Products operate and how they are employed by users. These are all proper computer science and engineering methods for analyzing the Accused Products and comparing them to the method and system claims of the ‘601 patent. Through this analysis I have been able to determine that the Accused Products either necessarily perform the accused steps or a majority of customers use the Accused Products to perform the accused steps. Mr. Hicks citation to Firewall logs and Router logs could be used in furtherance of such analysis, but based on my experience are not necessary to draw the conclusions that I have identified in my

report.

24. Mr. Hicks also asserts that there is “no actual evidence that any step of the claims 10 or 43 has ever been performed using any accused Fortinet product.” I disagree, as noted in my opening report, Fortinet’s customer EO Johnson configured the accused products that it purchased from Fortinet to perform web filtering through a transparent application layer proxy. (*See* EO Johnson.zip). Exhibit 1 provides the list of EO Johnson configuration files that enabled web filtering. Another example, as noted above, is Fortinet customer Qdoba, whose configuration files show that Qdoba’s Fortinet products were enabled to perform Web Filtering, VoIP Inspection, Antivirus, Email Filtering, and Data Leak Prevention. (*See* Exhibit 1 and Qdoba.zip). These configuration files corroborate Michael Xie’s testimony regarding the extent of use of UTM services by users of the Accused Products.

IV. CLAIMS 19 AND 57 OF THE ‘601 PATENT

25. Mr. Hicks states that the “accused products do not meet the “modified kernel” limitation of claims 19 and 57.” (Paragraph 19). This is incorrect. As described in my opening report and above, without a policy, the Accused Products cannot forward or transmit any information between a source and destination. Either by a default configuration or through user instructions, at least one policy is provided that sets the process by which a communications packet is transmitted through the Accused Products to the destination. These policies can be removed; when they are, the Accused Products’ default capability of not forwarding any information between a source and destination is reestablished.

26. In support of his analysis, Mr. Hicks relies on the factory default policy for routing and the phrases in the manual that mention that packets are “forwarded beyond the unit” to a

destination. (Paragraphs 7.3.6-7.3.8). Mr. Hicks asserts that these passages do not act in accordance with the requirements of claim 19. Mr. Hicks's reliance on the default policy settings for some of the Accused Products or proposed policy settings for initial setup are unavailing to his analysis. First, by default, the Accused Products perform Network Address Translation, which indicates that IP forwarding as described in the '601 patent is not utilized. Second, even if these preliminary settings have the meaning Mr. Hicks inappropriately attributes to them, Fortinet tells its customers to delete these preliminary policies because the network would otherwise be placed at risk. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, 338-339 ("It is a very broad policy and not recommended to keep on the system once initial setup and testing are complete. You will want to add more restrictive firewall policies to provide better network protection")) Fortinet instead tells its customers to create policies that assign application layer proxy process to port numbers and use those proxy processes to transparently establish communication sessions with the source and destination and transparently communicate information between the source and destination. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, p. 263-298 (policies for small office networks employing UTM), p. 299-330 (policies for library network protection employing UTM)). As acknowledged by Michael Xie, a majority of users employ this configuration.

27. Based on the opinions expressed in my opining report and as discussed above, contrary to Mr. Hicks's conclusion, my analysis shows that the Accused Products contain each and every limitation of claim 19 of the '601 patent.

V. CLAIM 29 OF THE '601 PATENT

28. With respect to element (a) of claim 29, Mr. Hicks states that "the correct structure

description for this element is: “a kernel, modified to accept for processing any TCP/IP packet having an encapsulation destination address that matches the device address of the gateway station and also modified to disable all IP forwarding, which receives and examines each packet to determine whether the encapsulation destination address equals the device address of the gateway station.” (Paragraph 7.4.4). While there are portions of this construction that I agree with, there are other requirements that Mr. Hicks improperly identifies as performing the claimed function. To the extent that Mr. Hicks claims that element (a) requires “a kernel modified to accept packets having an encapsulation destination address that matches the device address of the gateway station.” I agree with this requirement and believe that this is not materially different than the construction that I applied. However, Mr. Hicks’s requirements of “processing any TCP/IP packet” and “modified to disable all IP forwarding, which receives and examines each packet to determine whether the encapsulation destination address equals the device address of the gateway station” are improper. First, this construction is improper because neither requirement appears in element (a) or claim 29 for that matter. Second, this construction is improper because neither structure is necessary to perform the function of “accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway.” Third, in my opinion, Mr. Hicks is simply importing functional requirements that are not present in the claim.

29. As shown in my original report and discussed above with respect to claims 10 and 43, the Accused Products do have “means for accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway.” Moreover, even if Mr. Hicks’s construction of this limitation were to apply, for the reasons set forth with respect to claim 19, the Accused Products would nevertheless satisfy

the requirements of that construction.

30. With respect to element (b) of claim 29, Mr. Hicks states that the “proper structure description for this element is: “a kernel, modified to accept for processing any TCP/IP packet having an encapsulation destination address that matches the device address of the gateway station and also modified to disable all IP forwarding, which ignores the destination IP address as it examines the destination port of a packet to determine if the port number is bound to a process.” (Paragraph 7.4.9). To the extent that Mr. Hicks claims that element (b) requires “ a kernel, modified to determine whether there is a process bound to a destination port number of an accepted communications packet”, I agree with this requirement and believe that this is not materially different than the construction that I applied. However, the remainder of Mr. Hicks’s construction contains numerous errors. In particular:

- “accept for processing any TCP/IP packet having an encapsulation destination address that matches the device address of the gateway station”;
- “modified to disable all IP forwarding”;
- “ignores the destination IP address as it examines the destination port of a packet”; and
- “determine if the port number is bound to a process.”

First, these requirements are improper because they are not requirements or functions recited in element (b) of claim 29. As an example, Mr. Hicks’s construction requires a kernel to “determine if the port number is bound to a process.” However, this not the requirement of the claim, which states “determining whether there is a process bound [or assigned] to a destination port number of an accepted communications packet.” Also, Mr. Hicks’s proposed structure is

not described in the passages that he quotes. Second, Mr. Hick's construction improperly purposes the use of structure that is not necessary to perform the function of element (b). Third, Mr. Hicks construction improperly imports functional requirements in to element (b) that are not present. For instance, Mr. Hicks seeks to add "ignores the destination IP address as it examines the destination port of a packet." No such function is required by element (b). The only functional requirement is "determining whether there is a process bound to a destination port number of an accepted communications packet."

31. As shown in my original report and discussed above with respect to claims 10 and 43, the Accused Products do have "means for determining whether there is a process bound to a destination port number of an accepted communications packet." Moreover, even if Mr. Hicks's construction to require IP forwarding to be disabled were to apply, for the reasons set forth with respect to claim 19, the Accused Products would nevertheless satisfy the requirements of that construction.

32. With respect to element (c) of claim 29, Mr. Hicks states that the a "proper structure description for this element is: "a kernel, modified to accept for processing any TCP/IP packet having an encapsulation destination address that matches the device address of the gateway station and also modified to disable all IP forwarding, which drops the packet if no proxy process is bound to the destination port of the packet and no generic proxy process is bound to the destination port of the packet, and otherwise initiates a TCP or UDP session with the packet source IP address and delivers the packet to designated proxy process"." (Paragraph 7.4.15). I disagree with this analysis. Mr. Hick's definition improperly imports the following functional, which are not recited in element (c):

- "modified to accept for processing any TCP/IP packet having an

encapsulation destination address that matches the device address of the gateway station”;

- “modified to disable all IP forwarding”;
- “drops the packet if no proxy process is bound to the destination port of the packet and no generic proxy process is bound to the destination port of the packet”;
- “otherwise initiates a TCP or UDP session with the packet source IP address”;
- “delivers the packet to designated proxy process.”

33. The only function recited in element (c) is “establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet.” While the specification does describe the kernel in a preferred embodiment performing some of the functions identified above, those functions were not incorporated as a requirement for element (c). Mr. Hicks’s analysis seeks to improperly import these functions in to the requirements of element (c).

34. As shown in my original report and discussed above with respect to claims 10 and 43, the Accused Products do have “means for establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet.” Moreover, even if Mr. Hicks’s construction to require IP forwarding to be disabled were to apply, for the reasons set forth with respect to claim 19, the Accused Products would nevertheless satisfy the requirements of that construction.

VI. THE KEARL REPORT

35. I have reviewed a portion of the J.R. Kearl report, which states:

Second, Mr. Jarosz's entire "Income Approach" depends on his assumption that, absent the accused functionality, half of the customers who purchased an accused Fortinet product would not have done so. His sole basis for this assumption is the deposition testimony of Mr. Xie. However, Mr. Jarosz apparently either misunderstands or misrepresents the testimony of Mr. Xie. Mr. Jarosz states that the functionality that the patent enables is a "transparent application layer proxy."²⁷ (emphasis added) He cites Dr. Keromytis for the proposition that the ability to inspect data traffic at the application level enhances a UTM's capabilities.²⁸ Mr. Jarosz then cites to Mr. Xie's testimony that the majority of Fortinet customers who purchase a Fortigate product use at least one application process.²⁹ (emphasis added) Thus, Mr. Jarosz appears to be equating "application level proxies" (which is how he defines the functionality enabled by the patent) with "application processes."³⁰ However, Mr. Xie clearly stated in his deposition, as part of the same answer selectively quoted by Mr. Jarosz that he is not talking about proxies.³¹ Mr. Xie is making the simple point that, in the general computer world (and not specific to UTMs), a system consisting of only hardware and an operating system without applications would be of little value to users. In addition, as I understand it, even under Plaintiff's theory of infringement, Fortinet's products could offer some applications and functions or work with applications and not infringe. Thus, Mr. Jarosz has no support for his critical assumption that, absent the accused functionality, half of the FortiGate customers would not have purchased the product.

36. I have reviewed the testimony of Mr. Xie. In testimony, Mr. Xie acknowledged that at least a majority of purchasers use application layer processes.

- 1 Q. Do you think that purchasers of the
- 2 FortiGate products are likely to use the -- at least
- 3 one of the application layer processes?
- 4 A. I would say majority of the purchasers of
- 5 FortiGate product would use at least one of the --

6 the processes that offers those features.

(Xie Dep. Tr. 103:1-6).

37. Mr. Xie also acknowledged Fortinet could not offer the Accused Products without application layer processes.

6 Q. And if Fortinet could not offer these
7 application layer processes, would their FortiGate
8 product be competitive in the marketplace?
9 A. No, these application processes -- and
10 we're not talking about proxies or anything. But I
11 think in general computer science world, most of the
12 products sold are including these application layer
13 processes. So if none of them are running, the
14 FortiGate wouldn't offer any features, then I
15 wouldn't think anybody would use them.

(Xie Dep. Tr. 104:6-15).

38. While Mr. Xie tried to couch his comments as not being directed specifically to proxies, he later admitted that the application layer processes in the Accused Products are application layer proxies or processes that communicate with and are controlled by application layer proxies.

6 Q. And the -- which services that run on the
7 FortiGate products operate at the application layer?
8 A. So the FortiGate has a number of processes
9 which can receive and process packets.
10 Q. And which of those processes run at the
11 application layer?
12 A. So on the application layer, there were
13 several proxies that can receive and process
14 packets.
15 Q. What else?
16 A. I think we generally just refer to them as

17 proxies.

18 Q. Everything that runs at the application
19 layer is a proxy?

20 A. Nope. Everything run at the application
21 layer that can process and receive packets -- send
22 and receive packets, we call them -- inside the
23 FortiOS boundary is proxy.

24 Q. So, for example, antivirus. Is there an
25 antivirus process that runs on the FortiGate

...

1 products?

2 A. The antivirus is conducted in a process
3 that doesn't directly process packets, but it
4 communicate with the proxies of your sockets and
5 files.

6 Q. Okay. And the antivirus process runs at
7 the application layer, right?

8 A. That is correct.

9 Q. What other processes run at the application
10 layer?

11 A. There are too many that I could enumerate
12 here.

13 Q. Do as many as you can.

14 A. There's the Web server, there's the command
15 line server, Telnet server.

16 THE REPORTER: What was that?

17 THE WITNESS: Telnet server.

18 There's various routing processes. Yeah,
19 filtering processes. There -- there are a lot of
20 them.

...

8 MR. CUKOR: Q. So how important are these
9 application processes that you just identified to
10 the functionality of a UTM firewall?

11 A. Very important.

12 Q. How come?

13 A. Why they're important?

14 Q. Yes.

15 A. Because users expect those features that
16 are offered in these processes. If they don't run,
17 the user wouldn't get what they want.

(Xie Dep. Tr. 100:6-102:17

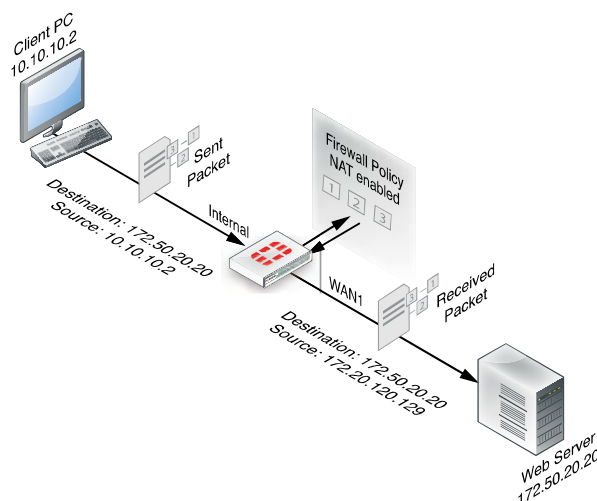
39. As noted in my opening report, the application layer processes are transparent application layer proxy processes within the scope of the claims of the '601 patent. Mr. Hicks does not dispute my analysis.

EXHIBIT J

1. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:

The purpose of firewalls is to act as secure gateways between a private (“protected”) and a potentially hostile network, such as the Internet. The accused products, manufactured by Fortinet, act as firewalls, as is described in Fortinet’s documentation (Handbook v3, page 183), website and source code.

Figure 6: Sender’s IP internal address translated to the FortiGate unit’s external address



(v2 FortiGate Fundamentals, p. 185)


A. So, assuming that the FortiGate device is configured properly to do some sort of filtering, the client -- client side person, that computer would open their browser and type in a website. This will initiate a communication, a TCP connection, to go to the -- to the server. The FortiGate will be sitting in the middle.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 6-11

[REDACTED]
FORTINET-NPS-SC 000066-000074

[378:381]

	<p>[REDACTED]</p> <p>[REDACTED]</p>
(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to the host, but encapsulating the packets with a hardware destination address that matches a device address of the gateway;	<p>A FortiGate security device operating under FortiOS is configured as a gateway, so that end devices use the destination IP address as if there were a communications path to the host, but encapsulating the packets with the MAC address of the gateway device. RFC 826 describes how this works for Ethernet-type networks, which is the most commonly used local area interconnection technology.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185</i> <i>FortiGate Version 4.0 MR2 Administration Guide, P. 173</i></p> <p><i>RFC 826, An Ethernet Address Resolution Protocol</i></p> <p>Q. Is there any address information contained in packets that are received by FortiGate device?</p> <p>A. Yes.</p> <p>Q. What kind of information?</p> <p>A. There's a MAC address, IP address.</p> <p><i>Crawford 30(b)(6) Dep. Trans. p. 126, lns. 7-11</i></p> <p>[REDACTED]</p> <p>FORTINET-NPS-SC 000066-000074</p> <p>[378:381]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>(Tab 38) FORT-NPS-SC0000023-27 (code that sets the MAC address of an Ethernet interface, for two different types of Ethernet interfaces --- 100Mbps and 1000Mbps)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601</p>

	<p>patent pertains, would understand that a data packet with the MAC address of the accused product and an IP address of the destination host is interchangeable or substitutable for this claim limitation / element; and this addressing contained in a data packet sent to the accused products element of the accused products does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
(b) accepting at the gateway communications packets from either network that are encapsulated with a hardware destination address which matches the device address of the gateway;	<p>The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185</i></p> <p>The Handbook v3, pages 707-708, describes, as an example, how a FortiGate device handles a packet transmitted from a web client to a web server and vice versa. Figure 69 on page 709 depicts graphically this process, which includes intercepting the packet, inspecting it through a variety of means, including a Proxy Inspection Engine that applies Antivirus and Web Filtering, and forwarding it if accepted by policy. Furthermore, the Handbook v3, pages 735-737, describes an example of a TCP connection between a client and server, to which various security policies are applied, showing how the packets are intercepted on either side and processed by FortiOS.</p>
	<p>Q. Is there any address information contained in packets that are received by FortiGate device?</p> <p>A. Yes.</p> <p>Q. What kind of information?</p> <p>A. There's a MAC address, IP address.</p> <p><i>Crawford 30(b)(6) Dep. Trans. p. 126, lns. 7-11</i></p>
	<p> FORTINET-NPS-SC 000066-000074</p> <p>[378:381]</p>

	<div data-bbox="451 191 1073 275" style="background-color: black; width: 383px; height: 40px; margin-bottom: 10px;"></div> <div data-bbox="436 306 1333 348" style="background-color: black; width: 552px; height: 20px;"></div> <p>(Tab 38) FORT-NPS-SC0000023-27 (code that sets the MAC address of an Ethernet interface, for two different types of Ethernet interfaces --- 100Mbps and 1000Mbps)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that a gateway with a kernel that accepts a data packet with the MAC address of the accused product is interchangeable or substitutable for this claim limitation / element; and this kernel that accepts a data packet with the MAC address of the accused product does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>(c) determining at the gateway whether there is a process bound to a destination port number of an accepted communications packet;</p>	<p>FortiOS determines whether there is a process bound or assigned to a destination port number of an accepted communications packet by matching the packet to a policy: <i>"When a firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet."</i> (FortiOS Handbook v2, pages 191, 196-197, and 231.)</p> <p>These policies determine, among other things, whether a proxy, as stated in the Handbook v3, pages 705-706, will process a packet:</p> <p><i>"The policy look up is where the FortiGate unit reviews the list of security policies which govern the flow of network traffic, from the first entry to the last, to find a match for the source and destination IP addresses and port numbers. The decision to accept or deny a packet, after being verified as a valid request within the stateful inspection, occurs here. A denied packet is discarded. An accepted packet will have further actions taken. If IPS is enabled, the packet will go to Flow-based inspection engine, otherwise it will go to the Proxy-based inspection engine. If no other UTM options are enabled, then the session was only subject to stateful inspection. If the action is accept, the packet will go to Source NAT to be ready to leave the FortiGate unit."</i></p>

The FortiGate device uses proxy processes to perform some of its security functionality. The Handbook v3, page 707, states:

“The proxy inspection engine is responsible for carrying out antivirus protection, email filtering (antispam), web filtering and data leak prevention. The proxy engine will process multiple packets to generate content before it is able to make a decision for a specific packet.”

“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).

“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-NPS 017058-59; FORT-NPS 017008).

“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).

“If the initial packet matches the firewall policy, the FortiGate unit performs the configured Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if
that initial TCP connection matches any of our policies.

Q. Okay. And if it does?


A. If it does match, then it will determine whether it's to pass that through or whether
it's going to – it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

These proxies are implemented as application-level (“user-level”) processes. This
can be seen in the FortiOS source code:


FORTINET-NPS-SC 000035-000036

[803:804]


[808:856]




FORTINET-NPS-SC 000043

[3:14]

INTRODUCTION

The redirect implementations take care of re-directing traffic to
the proxy and listening on the appropriate ports for the re-directed
traffic.

IMPLEMENTATIONS

fortitilter

This implementation relies on a fortifilter kernel helper to alter the session table to allow inbound connections. So, all this implementation does is take care of opening any required sockets to listen for re-directed connections. This is the implementation that should ship on a FortiGate.

[REDACTED]
FORTINET-NPS-SC 000039-000043

[9:16]

[REDACTED]

[124:126]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000037-000038

[4:5]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000066-000074

[58:67]

[REDACTED]

	<p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>FORTINET-NPS-SC 000110-000114</p> <p>[1711:1716]</p> <p>[REDACTED]</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the policies stored in the configuration file and written to the OS kernel of the accused products is interchangeable or substitutable for this claim limitation / element; and the manner in which accused products employ policies does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
(d) establishing transparently at the gateway a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the	<p>As noted above, the accused products examine a packet's source address, destination address and port number to determine if there is a policy and consequently an applicable transparent application layer proxy that is assigned to the port number.</p> <p>If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is transparently established between the source and the gateway (as indicated by creating an entry in the session table), otherwise the packet is dropped. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 193-194.) The creation of the first communication session between the source and the gateway, instead of the destination, would not be apparent to the initiator.</p>

destination port number, else dropping the packet;	If the accused products determine that there is not a policy assigned to the destination port number identified in the packet, then the packet will be dropped.
	<p><i>The Scanner Proxy</i></p> <p>The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will</p> <p>be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.</p> <p>FORT-NPS 169248-169249</p> <p>In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.</p> <p>From the point view of the client, this is what happens:</p> <ol style="list-style-type: none"> 1. client connects to server and makes request 2. server sends back response. <p>In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.</p> <p>FORT-NPS 165878</p> <p>“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).</p> <p>“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-</p>

NPS 017058-59; FORT-NPS 017008).

“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).

“If the initial packet matches the firewall policy, the FortiGate unit performs the configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if that initial TCP connection matches any of our policies.

Q. Okay. And if it does?

A. If it does match, then it will determine whether it's to pass that through or whether it's going to -- it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

This is also supported by the source code, which clearly indicates that FortiOS manages the two connections separately.

[REDACTED]

FORTINET-NPS-SC 000066-000074

[4:9]

[REDACTED]

[196:200]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[37:41]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000115-000116

[36:69]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000117-000118

[22:51]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

relevant:

[REDACTED]

FORTINET-NPS-SC 000109

(Tab 4)

FORT-NPS-SC0000641 (receive a connection at the IMD proxy)

(Tab 5)

FORT-NPS-SC0000622 (receive a client connection, for the NNTP proxy)

(Tab 15)

	<p>FORT-NPS-SC0000409 (receive a client connection, for the SMTP proxy)</p> <p>(Tab 22)</p> <p>FORT-NPS-SC0000338 (receive a client connection, for the POP3 proxy)</p> <p>(Tab 24)</p> <p>FORT-NPS-SC0000298-300 (receive a client connection, IMAP proxy)</p> <p>(Tab 27)</p> <p>FORT-NPS-SC0000252-253 (receive a client connection, FTP proxy)</p> <p>FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the transparent proxies or worker proxies of the accused products is interchangeable or substitutable for this claim limitation / element; and that these transparent proxies or worker proxies do not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>(e) establishing transparently at the gateway a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and</p>	<p>Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet. The Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 186-187 and 193 state:</p> <p><i>"Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions."</i></p> <p>The creation of the second communication session between the destination and the gateway, instead of between the source and the destination, would not be apparent to the initiator.</p>

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

The FortiOS source code also shows that :

[REDACTED]

FORTINET-NPS-SC 000066-000074

[196:200]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000058-000063

[1158:1422]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[43:48]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000110-000114

[59:63]

[REDACTED]

[1711:1719]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000140-000145

[1456:1476]

[REDACTED]

[REDACTED]

[REDACTED]

[3190:3194]

[REDACTED]

relevant:

[REDACTED]

FORTINET-NPS-SC 000109

(Tab 5)

FORT-NPS-SC0000611-613 (connect to the server, for the NNTP proxy)

(Tab 15)

FORT-NPS-SC0000396 (SMTP proxy connects to the server)

(Tab 22)

FORT-NPS-SC0000327-330 (POP3 proxy connects to the server)

(Tab 24)

FORT-NPS-SC0000287-290 (IMAP proxy connects to the server)

(Tab 27)

FORT-NPS-SC0000238-241 (connect to the server, for FTP proxy)

FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)

	<p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the transparent proxies or worker proxies of the accused products is interchangeable or substitutable for this claim limitation / element; and that these transparent proxies or worker proxies do not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>(f) transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.</p>	<p>Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. The transfer of data between each communication session through the proxy process would not be apparent to the initiator.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.</i></p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>Proxies</p> <p>Application Proxies</p> <p>Each protocol that can be inspected has a dedicated transparent proxy in the FortiOS architecture. This proxy sits between the client and the server intercepting all connections (requests and responses).</p> <p>Tasks performed by the protocol proxies include:</p> <ul style="list-style-type: none"> • Making decisions <p>The proxy, in cooperation with the inspection daemons (antivirus, antisipam or webfiltering) is responsible for making the decision to buffer, pass or block data passing through the FortiGate based on the policies in place.</p> </div> <p>(Course 301-v4.0 Secured Network Deployment and Virtual Private Networks, p. 281)</p>

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

traffic such as incoming traffic through VIP or Port Forwarding; redirect table [REDACTED] is for those traffic that need to go through our transparent proxies, such as anti-virus engine, for further processing;

FORT-NPS 164710

A. Okay. The transparent proxy, the user does not need to configure their browser, so they'll just use their browser, their computer goes on the network with the -- and it will make a request to try to visit the website, and FortiGate will be in the middle and can intercept that communication. And the content of the communication can be

buffered and given to another program to apply the antivirus filter on it. And, again, if everything is okay, then it can either let the trafficking through or block it or perform other actions on it.

Crawford 30(b)(6) Dep. Trans. p. 92 lns. 7-17

This can be seen in the FortiOS source code:

[REDACTED]
FORTINET-NPS-SC 000066-000074

[201:204]

[REDACTED]

[269:275]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000119-000124

[50:54]

[REDACTED]

[250:258]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000075-000077

[32:96]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000140-000145

[3997:4013]

/*

* We've just received a ClientHello from the client.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000064-000065

[862:867]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000015-000034

[4:5]

[REDACTED]

[24:25]

[REDACTED]

[843:864]

[REDACTED]

[...]

[REDACTED]

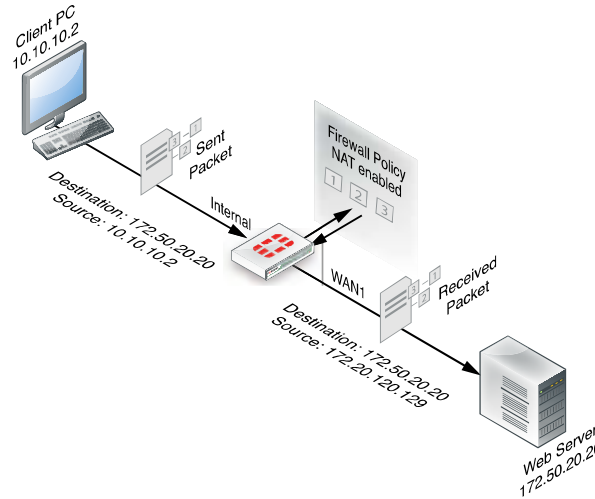
	<p>(Tab 22) FORT-NPS-SC0000336 (POP3 proxy code moving data across connections)</p> <p>(Tab 5) FORT-NPS-SC0000619-620 (NNTP proxy code moving data across connections)</p> <p>(Tab 15) FORT-NPS-SC0000404-405 (SMTP proxy code moving data across connections)</p> <p>(Tab 24) FORT-NPS-SC0000296 (IMAP proxy code moving data across connections)</p> <p>(Tab 27) FORT-NPS-SC0000249 (FTP proxy code moving data across connections)</p> <p>(Tab 29) FORT-NPS-SC0000210-211 (general code, across all proxies, for reading from/writing to connections to client and server)</p> <p>(Tab 31) FORT-NPS-SC0000199-201 (code for passing sockets from the acceptor to a proxy) Same also on Tab 47, FORT-NPS-SC0000856-858</p> <p>(Tab 44) FORT-NPS-SC0000867-868 (code for returning content scanning results to the requesting proxy)</p> <p>(Tab 45) FORT-NPS-SC0000974 proxy acceptor / proxy worker initialization code</p> <p>(Tab 48) Worker code</p> <p>(Tab 52) Acceptor code.</p>
	<p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the original transparent application layer proxies used with the accused products or the transparent application layer proxies</p>

	<p>that utilize a transparent proxy that controls or instructs a scan unit to perform application layer filtering with the accused products is interchangeable or substitutable for this claim limitation / element; and that neither the original transparent application layer proxies or the subsequent transparent application layer proxies play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>43. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the accepted communications packet is received at the gateway from the private network, wherein the accepted packet is addressed directly to a host on the potentially hostile network as if there were a communications path to the host and is encapsulated with the hardware destination address that matches the device address of the gateway, and wherein transparently moving data comprises passing communications packets to at least one proxy process that is configured to operate at an application layer of the gateway.</p>	<p>As explained and cited above in claim 1, packets received from a private network communicating with an accused product are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device.</p> <p>Further as explained and cited above in claim 1, the accused products process the communications between the sender and destination through transparent application layer proxy processes, including email filters, anti virus filters, web filters and data leak prevention. The transfer of data through these application layer proxy processes would not be apparent to the initiator.</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the original transparent application layer proxies used with the accused products or the transparent application layer proxies that utilize a transparent proxy that controls or instructs a scan unit to perform application layer filtering with the accused products is interchangeable or substitutable for this claim limitation / element; and that neither the original transparent application layer proxies or the subsequent transparent application layer proxies play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>

10. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:

The purpose of firewalls is to act as secure gateways between a private (“protected”) and a potentially hostile network, such as the Internet. The accused products, manufactured by Fortinet, act as firewalls, as is described in Fortinet’s documentation (Handbook v3, page 183), website and source code.

Figure 6: Sender's IP internal address translated to the FortiGate unit's external address



(v2 FortiGate Fundamentals, p. 185)

A. So, assuming that the FortiGate device is configured properly to do some sort of filtering, the client -- client side person, that computer would open their browser and type in a website. This will initiate a communication, a TCP connection, to go to the -- to the server. The FortiGate will be sitting in the middle.


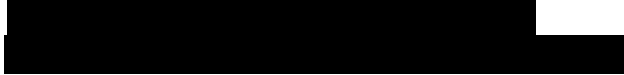
Crawford 30(b)(6) Dep. Trans. p. 99, lns. 6-11

[REDACTED]
FORTINET-NPS-SC 000066-000074

[378:381]

[REDACTED]
[REDACTED]

[REDACTED]

<p>(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to host, but encapsulating the packets with a hardware destination address that matches a device address of the gateway;</p>	<p>A FortiGate security device operating under FortiOS is configured as a gateway, so that end devices use the destination IP address as if there were a communications path to the host, but encapsulating the packets with the MAC address of the gateway device. RFC 826 describes how this works for Ethernet-type networks, which is the most commonly used local area interconnection technology.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185</i> <i>FortiGate Version 4.0 MR2 Administration Guide, P. 173</i></p> <p><i>RFC 826, An Ethernet Address Resolution Protocol</i></p>
	<p>Q. Is there any address information contained in packets that are received by FortiGate device?</p> <p>A. Yes.</p> <p>Q. What kind of information?</p> <p>A. There's a MAC address, IP address.</p> <p><i>Crawford 30(b)(6) Dep. Trans. p. 126, lns. 7-11</i></p>
	<p> FORTINET-NPS-SC 000066-000074</p> <p>[378:381]</p> <p></p> <p>Logically the client, proxy and server would be on different machines.</p> <p>(Tab 38) FORT-NPS-SC0000023-27 (code that sets the MAC address of an Ethernet interface, for two different types of Ethernet interfaces --- 100Mbps and 1000Mbps)</p>

	<p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that a data packet with the MAC address of the accused product and an IP address of the destination host is interchangeable or substitutable for this claim limitation / element; and this addressing contained in a data packet sent to the accused products element of the accused products does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>(b) accepting from either network all TCP/IP packets that are encapsulated with a hardware destination address which matches the device address of the gateway;</p>	<p>The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185</i></p> <p>The Handbook v3, pages 707-708, describes, as an example, how a FortiGate device handles a packet transmitted from a web client to a web server and vice versa. Figure 69 on page 709 depicts graphically this process, which includes intercepting the packet, inspecting it through a variety of means, including a Proxy Inspection Engine that applies Antivirus and Web Filtering, and forwarding it if accepted by policy. Furthermore, the Handbook v3, pages 735-737, describes an example of a TCP connection between a client and server, to which various security policies are applied, showing how the packets are intercepted on either side and processed by FortiOS.</p> <p>Q. Is there any address information contained in packets that are received by FortiGate device?</p> <p>A. Yes.</p> <p>Q. What kind of information?</p>

	<p>A. There's a MAC address, IP address.</p> <p><i>Crawford 30(b)(6) Dep. Trans. p. 126, lns. 7-11</i></p> <p>[REDACTED]</p> <p>FORTINET-NPS-SC 000066-000074</p> <p>[378:381]</p> <p>[REDACTED]</p> <p>Logically the client, proxy and server would be on different machines.</p> <p>(Tab 38)</p> <p>FORT-NPS-SC0000023-27 (code that sets the MAC address of an Ethernet interface, for two different types of Ethernet interfaces --- 100Mbps and 1000Mbps)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that a gateway with a kernel that accepts a data packet with the MAC address of the accused product is interchangeable or substitutable for this claim limitation / element; and this kernel that accepts a data packet with the MAC address of the accused product does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
(c) determining whether there is a proxy process bound to a port for serving a destination port number of an accepted TCP/IP	<p>FortiOS determines whether there is a process bound or assigned to a destination port number of an accepted communications packet by matching the packet to a policy: <i>"When a firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet."</i> (FortiOS Handbook v2, pages 191, 196-197, and 231.)</p>

packet;	<p>These policies determine, among other things, whether a proxy, as stated in the Handbook v3, pages 705-706, will process a packet:</p> <p><i>“The policy look up is where the FortiGate unit reviews the list of security policies which govern the flow of network traffic, from the first entry to the last, to find a match for the source and destination IP addresses and port numbers. The decision to accept or deny a packet, after being verified as a valid request within the stateful inspection, occurs here. A denied packet is discarded. An accepted packet will have further actions taken. If IPS is enabled, the packet will go to Flow-based inspection engine, otherwise it will go to the Proxy-based inspection engine. If no other UTM options are enabled, then the session was only subject to stateful inspection. If the action is accept, the packet will go to Source NAT to be ready to leave the FortiGate unit.”</i></p> <p>The FortiGate device uses proxy processes to perform some of its security functionality. The Handbook v3, page 707, states:</p> <p><i>“The proxy inspection engine is responsible for carrying out antivirus protection, email filtering (antispam), web filtering and data leak prevention. The proxy engine will process multiple packets to generate content before it is able to make a decision for a specific packet.”</i></p> <p>“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).</p> <p>“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-NPS 017058-59; FORT-NPS 017008).</p> <p>“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).</p> <p>“If the initial packet matches the firewall policy, the FortiGate unit performs the configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).</p> <p>“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).</p>
---------	--

"If no policy matches, the connection is dropped." (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if that initial TCP connection matches any of our policies.

Q. Okay. And if it does?

A. If it does match, then it will determine whether it's to pass that through or whether it's going to -- it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

These proxies are implemented as application-level ("user-level") processes. This can be seen in the FortiOS source code:

[REDACTED]
FORTINET-NPS-SC 000035-000036

[803:804]

[808:856]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000043

[3:14]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000039-000043

[9:16]

[REDACTED]

[124:126]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000037-000038

[4:5]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000066-000074

[58:67]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000110-000114

[1711:1716]

[REDACTED]

To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the policies stored in the configuration file

	<p>and written to the OS kernel of the accused products is interchangeable or substitutable for this claim limitation / element; and the manner in which accused products employ policies does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
(d) establishing a first communications session with a source address/source port number of the accepted TCP/IP packet if there is proxy process bound to the port for serving the destination port number, else dropping the packet;	<p>As noted above, the accused products examine a packet's source address, destination address and port number to determine if there is a policy and consequently an applicable transparent application layer proxy that is assigned to the port number.</p> <p>If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is transparently established between the source and the gateway (as indicated by creating an entry in the session table), otherwise the packet is dropped. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 193-194.) The creation of the first communication session between the source and the gateway, instead of the destination, would not be apparent to the initiator.</p> <p>If the accused products determine that there is not a policy assigned to the destination port number identified in the packet, then the packet will be dropped.</p> <p><i>The Scanner Proxy</i></p> <p>The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will</p> <p>be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.</p> <p>FORT-NPS 169248-169249</p>

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).

“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-NPS 017058-59; FORT-NPS 017008).

“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).

“If the initial packet matches the firewall policy, the FortiGate unit performs the configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if that initial TCP connection matches any of our policies.

Q. Okay. And if it does?

A. If it does match, then it will determine whether it's to pass that through or whether it's going to -- it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

This is also supported by the source code, which clearly indicates that FortiOS manages the two connections separately.

[REDACTED]

FORTINET-NPS-SC 000066-000074

[4:9]

[REDACTED]

[196:200]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000119-000124

[37:41]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000115-000116

[36:69]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000117-000118

[22:51]

relevant:

FORTINET-NPS-SC 000109

(Tab 4)

FORT-NPS-SC0000641 (receive a connection at the IMD proxy)

(Tab 5)

FORT-NPS-SC0000622 (receive a client connection, for the NNTP proxy)

(Tab 15)

FORT-NPS-SC0000409 (receive a client connection, for the SMTP proxy)

(Tab 22)

FORT-NPS-SC0000338 (receive a client connection, for the POP3 proxy)

(Tab 24)

FORT-NPS-SC0000298-300 (receive a client connection, IMAP proxy)

(Tab 27)

FORT-NPS-SC0000252-253 (receive a client connection, FTP proxy)

FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)

To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the transparent proxies or worker proxies of the accused products is interchangeable or substitutable for this claim limitation /

	<p>element; and that these transparent proxies or worker proxies do not play a role which is substantially different.</p>
--	---

	<p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
--	---

(e) determining if the source address/source port number of the accepted packet is permitted to communicate with a destination address/destination port number of the accepted packet by referencing a rule base, and dropping the packet if a permission rule cannot be located;

A FortiGate security device denies traffic between source and destination unless a policy permits the traffic. The FortiGate security device receives the first packet in a communications session and checks the policy rule base to determine whether the communication is permitted.

Handbook v3, page 185 states:

*“The FortiGate unit performs three types of security inspection:
stateful inspection, that provides individual packet-based security within a basic session state
flow-based inspection, that buffers packets and uses pattern matching to identify security threats
proxy-based inspection, that reconstructs content passing through the FortiGate unit and inspects the content for security threats.”*

Therefore, proxy-based inspection performs its own determination on whether a particular session is allowed, based on the specific functionality implemented by each proxy. As a result of this determination, a packet/connection may not be allowed to continue, as described in the Handbook v3, page 186:

*“3 If nothing comes from the stateful inspection engine, then the packet travels to the UTM scanning process. This process may have either a flow-based or proxy-based inspection engine that also processes the packet.
4 If nothing matches the UTM rules, the packet then travels to other processing steps, which include:
IPsec
NAT (Source NAT)
Routing
Internal Interface
5 After step 4 is finished, the packet travels out of the internal interface of the FortiGate unit, heading towards its final destination, the internal network. This is referred to as Egress.”*

If the UTM scanning process (i.e., the proxy-based inspection) determines there is a security threat, the packet is not allowed to travel to other processing steps. Each proxy uses its own rule set that determines whether a particular communication is acceptable. For example, the Antivirus proxy uses a database of virus signatures.

	<p>[REDACTED]</p> <p>[151:156]</p> <p>[REDACTED]</p> <p>[REDACTED]</p> <p>FORTINET-NPS-SC000040-41 (create a “pinhole” policy at the firewall to redirect traffic that hits that pinhole up to the IM proxy, for direct client-to-client IM connections)</p> <p>FORTINET-NPS-SC000059 (Validate a session, drop connections if not possible)</p> <p>FORTINET-NPS-SC000078 (Authenticate user, otherwise drop connection)</p> <p>FORTINET-NPS-SC000086-87 (Allow user to continue the telnet session if authenticated, otherwise require authentication; if that fails, drop connection and do not connect to the user-intended server destination)</p> <p>FORTINET-NPS-SC000097 (Same as previous, for HTTP)</p> <p>FORTINET-NPS-SC000107 (Create a new session that indicates a user is authenticated)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the ‘601 patent pertains, would understand that the policies stored in the configuration file and written to the OS kernel of the accused products of the accused products is interchangeable or substitutable for this claim limitation / element; and that these manner in which accused products employ policies do not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet’s expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
(f) establishing a second communications	Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with

<p>session with the destination address/destination port number of the accepted TCP/IP packet if a first communications session is established and the permission rule is located; and</p>	<p>the accepted communications packet. The Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 186-187 and 193 state:</p> <p><i>“Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions.”</i></p> <p>The creation of the second communication session between the destination and the gateway, instead of between the source and the destination, would not be apparent to the initiator.</p> <p><i>The Scanner Proxy</i></p> <p>The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will</p> <p>be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.</p> <p>FORT-NPS 169248-169249</p> <p>In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.</p> <p>From the point view of the client, this is what happens:</p> <ol style="list-style-type: none"> 1. client connects to server and makes request 2. server sends back response. <p>In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.</p>
--	--

FORT-NPS 165878

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

The FortiOS source code also shows that :

[REDACTED]
FORTINET-NPS-SC 000066-000074

[196:200]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000058-000063

[1158:1422]

static int connPostSetup(int aConnected, connection_t* aConn, const char

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[43:48]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000110-000114

[59:63]

[REDACTED]

[1711:1719]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000140-000145

[1456:1476]

[REDACTED]

[REDACTED]

[REDACTED]

[3190:3194]

[REDACTED]

relevant:

[REDACTED]

FORTINET-NPS-SC 000109

(Tab 5)

FORT-NPS-SC0000611-613 (connect to the server, for the NNTP proxy)

(Tab 15)

	<p>FORT-NPS-SC0000396 (SMTP proxy connects to the server)</p> <p>(Tab 22)</p> <p>FORT-NPS-SC0000327-330 (POP3 proxy connects to the server)</p> <p>(Tab 24)</p> <p>FORT-NPS-SC0000287-290 (IMAP proxy connects to the server)</p> <p>(Tab 27)</p> <p>FORT-NPS-SC0000238-241 (connect to the server, for FTP proxy)</p> <p>FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the transparent proxies or worker proxies of the accused products is interchangeable or substitutable for this claim limitation / element; and that these transparent proxies or worker proxies do not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>(g) transparently moving data associated with each subsequent TCP/IP packet between the respective first and second communications sessions, whereby the first session communicates with</p>	<p>Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. The transfer of data between each communication session through the proxy process would not be apparent to the initiator.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.</i></p>

the source and the second session communicates with the destination using the data moved between the first and second sessions.

Proxies

Application Proxies

Each protocol that can be inspected has a dedicated transparent proxy in the FortiOS architecture. This proxy sits between the client and the server intercepting all connections (requests and responses).

Tasks performed by the protocol proxies include:

- Making decisions

The proxy, in cooperation with the inspection daemons (antivirus, antispam or webfiltering) is responsible for making the decision to buffer, pass or block data passing through the FortiGate based on the policies in place.

(Course 301-v4.0 Secured Network Deployment and Virtual Private Networks, p. 281)

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

traffic such as incoming traffic through VIP or Port Forwarding; redirect table [REDACTED] is for those traffic that need to go through our transparent proxies, such as anti-virus engine, for further processing;

FORT-NPS 164710

A. Okay. The transparent proxy, the user does not need to configure their browser, so they'll just use their browser, their computer goes on the network with the -- and it will make a request to try to visit the website, and FortiGate will be in the middle and can intercept that communication. And the content of the communication can be buffered and given to another program to apply the antivirus filter on it. And, again, if everything is okay, then it can either let the trafficking through or block it or perform other actions on it.

Crawford 30(b)(6) Dep. Trans. p. 92 Ins. 7-17

This can be seen in the FortiOS source code:

[REDACTED]
FORTINET-NPS-SC 000066-000074

[201:204]

[REDACTED]

[REDACTED]

[269:275]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[50:54]

[REDACTED]

[250:258]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000075-000077

[32:96]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000140-000145

[3997:4013]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000064-000065

[862:867]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000015-000034

[4:5]

[REDACTED]

[24:25]

[REDACTED]

[843:864]

[REDACTED]

[REDACTED]

[REDACTED]

(Tab 22)

FORT-NPS-SC0000336 (POP3 proxy code moving data across connections)

(Tab 5)

FORT-NPS-SC0000619-620 (NNTP proxy code moving data across connections)

(Tab 15)

FORT-NPS-SC0000404-405 (SMTP proxy code moving data across connections)

(Tab 24)

FORT-NPS-SC0000296 (IMAP proxy code moving data across connections)

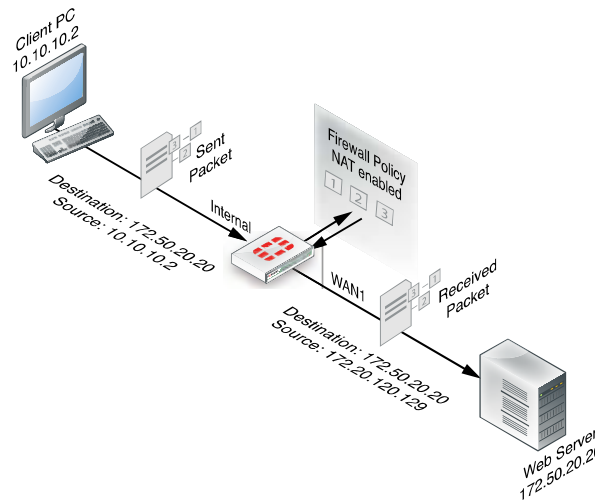
(Tab 27)

	<p>FORT-NPS-SC0000249 (FTP proxy code moving data across connections)</p> <p>(Tab 29) FORT-NPS-SC0000210-211 (general code, across all proxies, for reading from/writing to connections to client and server)</p> <p>(Tab 31) FORT-NPS-SC0000199-201 (code for passing sockets from the acceptor to a proxy) Same also on Tab 47, FORT-NPS-SC0000856-858</p> <p>(Tab 44) FORT-NPS-SC0000867-868 (code for returning content scanning results to the requesting proxy)</p> <p>(Tab 45) FORT-NPS-SC0000974 proxy acceptor / proxy worker initialization code</p> <p>(Tab 48) Worker code</p> <p>(Tab 52) Acceptor code.</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the original transparent application layer proxies used with the accused products or the transparent application layer proxies that utilize a transparent proxy that controls or instructs a scan unit to perform application layer filtering with the accused products is interchangeable or substitutable for this claim limitation / element; and that neither the original transparent application layer proxies or the subsequent transparent application layer proxies play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling. discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>19. Apparatus for providing a secure gateway for data exchanges between a</p>	<p>The purpose of firewalls is to act as secure gateways between a private ("protected") and a potentially hostile network, such as the Internet. The accused products, manufactured by Fortinet, act as firewalls, as is described in Fortinet's documentation (Handbook v3, page 183), website and source code.</p>

private network and a potentially hostile network, comprising in combination:

a gateway station adapted for connection to a telecommunications connection with each of the private network and the potentially hostile network;

Figure 6: Sender's IP internal address translated to the FortiGate unit's external address



(v2 FortiGate Fundamentals, p. 185)

A. So, assuming that the FortiGate device is configured properly to do some sort of filtering, the client -- client side person, that computer would open their browser and type in a website. This will initiate a communication, a TCP connection, to go to the -- to the server. The FortiGate will be sitting in the middle.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 6-11

[REDACTED]
FORTINET-NPS-SC 000066-000074

[378:381]

[REDACTED]
[REDACTED]

[REDACTED]

an operating system executable by the gateway station, a

FortiOS is an operating system executable at the FortiGate gateways. The kernel is operating on a modified Linux kernel to perform the elements recited in this claim.

<p>kernel of the operating system having been modified so that the operating system:</p>	<p>http://www.fortinet.com/products/fortigate/ Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 177, 184, 185</p> <p>Q. And what operating system does the FortiGate device --A. We have a variation of the Linux kernel. Q. Of the Linux kernel? A. Yes.</p> <p><i>Crawford 30(b)(6) Dep. Trans. p. 42, lns. 19-23.</i></p> <p>[REDACTED] FORTINET-NPS-SC 000066-000074</p> <p>[378:381]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>a) cannot forward any communications packet from the private network to the potentially hostile network or from the potentially hostile network to the private network; and</p>	<p>The FortiOS kernel is modified so that packets with a destination IP address other than the gateway are not forwarded from the private network to the potentially hostile network or from the potentially hostile network to the private network without processing by the gateway.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185</i> <i>FortiGate Version 4.0 MR2 Administration Guide, P. 173</i></p> <p>Furthermore, in order for any of the accused products to be permitted to transmit communications packets between a source and destination, a policy needs to be established. Without a policy, the accused products cannot forward communications packets in between a source and a destination.</p> <p>“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-NPS 017058-59; FORT-NPS 017008).</p> <p>“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).</p> <p>“If the initial packet matches the firewall policy, the FortiGate unit performs the</p>

configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

Q. Is there any particular configuration or modifications that need to be made to a FortiGate to allow it to transfer any particular type of protocol,

A. You need a policy.

Crawford 30(b)(6) Dep. Trans. p. 50,, lns. 23-25, p. 51, ln. 2

Q. What happens if it doesn't match a policy?

A. The communication will be terminated.

Crawford 30(b)(6) Dep. Trans. p. 101, lns. 12-13

	<p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the policies stored in the configuration file and written to the OS kernel of the accused products is interchangeable or substitutable for this claim limitation / element; and the manner in which accused products employ policies does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>b) will accept for processing any communications packet from either of the private network and the potentially hostile network provided that the packet is encapsulated with a hardware destination address that matches the device address of the gateway station on the respective network; and</p>	<p>The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185</i></p> <p>The Handbook v3, pages 707-708, describes, as an example, how a FortiGate device handles a packet transmitted from a web client to a web server and vice versa. Figure 69 on page 709 depicts graphically this process, which includes intercepting the packet, inspecting it through a variety of means, including a Proxy Inspection Engine that applies Antivirus and Web Filtering, and forwarding it if accepted by policy. Furthermore, the Handbook v3, pages 735-737, describes an example of a TCP connection between a client and server, to which various security policies are applied, showing how the packets are intercepted on either side and processed by FortiOS.</p>
	<p>Q. Is there any address information contained in packets that are received by FortiGate device?</p> <p>A. Yes.</p> <p>Q. What kind of information?</p> <p>A. There's a MAC address, IP address.</p> <p><i>Crawford 30(b)(6) Dep. Trans. p. 126, lns. 7-11</i></p>

	<div data-bbox="418 310 802 348" style="background-color: black; width: 236px; height: 18px; margin-bottom: 5px;"></div> <p data-bbox="418 352 907 384">FORTINET-NPS-SC 000066-000074</p> <p data-bbox="418 426 550 457">[378:381]</p> <div data-bbox="451 491 1073 569" style="background-color: black; width: 383px; height: 37px; margin-bottom: 5px;"></div> <div data-bbox="435 602 1334 642" style="background-color: black; width: 554px; height: 19px;"></div> <p data-bbox="418 720 1498 825">(Tab 38) FORT-NPS-SC0000023-27 (code that sets the MAC address of an Ethernet interface, for two different types of Ethernet interfaces --- 100Mbps and 1000Mbps)</p> <p data-bbox="418 915 1511 1241">To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the ‘601 patent pertains, would understand that the policies stored in the configuration file and written to the OS kernel of the accused products is interchangeable or substitutable for this claim limitation / element; and the manner in which accused products employ policies does not play a role which is substantially different.</p> <p data-bbox="418 1276 1393 1381">I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet’s expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p data-bbox="107 1434 391 1829">at least one proxy process executable by the gateway station, the at least one proxy process being adapted to transparently initiate a first communications session with a source of an initial data packet accepted by</p>	<p data-bbox="418 1434 1511 1539">As noted above, the accused products examine a packet’s source address, destination address and port number to determine if there is a policy and consequently an applicable transparent application layer proxy that is assigned to the port number.</p> <p data-bbox="418 1581 1511 1791">If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is transparently established between the source and the gateway (as indicated by creating an entry in the session table), otherwise the packet is dropped. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 193-194.) The creation of the first communication session between the source and the gateway, instead of the destination, would not be apparent to the initiator.</p>

<p>the operating system and to transparently initiate a second communications session with a destination of the packet without intervention by the source, and to transparently pass the data portion of packets received by the first communications session to the second communications session and to pass the data portion of packets received by the second communications session to the first communications session, whereby the first session communicates with the source using data from the second session and the second session communicates with the destination using data received from the first session.</p>	<p>If the accused products determine that there is not a policy assigned to the destination port number identified in the packet, then the packet will be dropped.</p> <p><i>The Scanner Proxy</i></p> <p>The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.</p> <p>FORT-NPS 169248-169249</p> <p>In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.</p> <p>From the point view of the client, this is what happens:</p> <ol style="list-style-type: none"> 1. client connects to server and makes request 2. server sends back response. <p>In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.</p> <p>FORT-NPS 165878</p> <p>“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).</p> <p>“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-</p>
--	--

NPS 017058-59; FORT-NPS 017008).

“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).

“If the initial packet matches the firewall policy, the FortiGate unit performs the configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if that initial TCP connection matches any of our policies.

Q. Okay. And if it does?

A. If it does match, then it will determine whether it's to pass that through or whether it's going to -- it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

This is also supported by the source code, which clearly indicates that FortiOS manages the two connections separately.

[REDACTED]

FORTINET-NPS-SC 000066-000074

[4:9]

[REDACTED]

[196:200]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[37:41]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000115-000116

[36:69]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000117-000118

[22:51]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

relevant:

[REDACTED]
FORTINET-NPS-SC 000109

(Tab 4)

FORT-NPS-SC0000641 (receive a connection at the IMD proxy)

(Tab 5)

FORT-NPS-SC0000622 (receive a client connection, for the NNTP proxy)

	<p>(Tab 15) FORT-NPS-SC0000409 (receive a client connection, for the SMTP proxy)</p> <p>(Tab 22) FORT-NPS-SC0000338 (receive a client connection, for the POP3 proxy)</p> <p>(Tab 24) FORT-NPS-SC0000298-300 (receive a client connection, IMAP proxy)</p> <p>(Tab 27) FORT-NPS-SC0000252-253 (receive a client connection, FTP proxy)</p> <p>FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)</p>
	<p>Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet. The Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 186-187 and 193 state:</p> <p><i>“Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions.”</i></p> <p>The creation of the second communication session between the destination and the gateway, instead of between the source and the destination, would not be apparent to the initiator.</p>
	<p>The Scanner Proxy</p> <p>The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will</p>

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

The FortiOS source code also shows that :

[REDACTED]

FORTINET-NPS-SC 000066-000074

[196:200]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000058-000063

[1158:1422]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[43:48]

[REDACTED]g

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000110-000114

[59:63]

[REDACTED]

[1711:1719]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000140-000145

[1456:1476]

[REDACTED]

[REDACTED]

[REDACTED]

[3190:3194]

relevant:

FORTINET-NPS-SC 000109

(Tab 5)

FORT-NPS-SC0000611-613 (connect to the server, for the NNTP proxy)

(Tab 15)

FORT-NPS-SC0000396 (SMTP proxy connects to the server)

(Tab 22)

FORT-NPS-SC0000327-330 (POP3 proxy connects to the server)

(Tab 24)

FORT-NPS-SC0000287-290 (IMAP proxy connects to the server)

(Tab 27)

FORT-NPS-SC0000238-241 (connect to the server, for FTP proxy)

FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)

Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. The transfer of data between each communication session through the proxy process would not be apparent to the initiator.

Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.

Proxies

Application Proxies

Each protocol that can be inspected has a dedicated transparent proxy in the FortiOS architecture. This proxy sits between the client and the server intercepting all connections (requests and responses).

Tasks performed by the protocol proxies include:

- Making decisions

The proxy, in cooperation with the inspection daemons (antivirus, antispam or webfiltering) is responsible for making the decision to buffer, pass or block data passing through the FortiGate based on the policies in place.

(Course 301-v4.0 Secured Network Deployment and Virtual Private Networks, p. 281)

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

traffic such as incoming traffic through VIP or Port Forwarding; redirect table [REDACTED] is for those traffic that need to go through our transparent proxies, such as anti-virus engine, for further processing;

FORT-NPS 164710

A. Okay. The transparent proxy, the user does not need to configure their browser, so they'll just use their browser, their computer goes on the network with the -- and it will make a request to try to visit the website, and FortiGate will be in the middle and can intercept that communication. And the content of the communication can be buffered and given to another program to apply the antivirus filter on it. And, again, if everything is okay, then it can either let the trafficking through or block it or perform other actions on it.

Crawford 30(b)(6) Dep. Trans. p. 92 lns. 7-17

This can be seen in the FortiOS source code:

[REDACTED]
FORTINET-NPS-SC 000066-000074

[201:204]

[REDACTED]

[269:275]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[50:54]

[REDACTED]

[250:258]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000075-000077

[32:96]

[REDACTED]

	<div data-bbox="418 197 467 239">[REDACTED]</div> <div data-bbox="418 268 1425 348">[REDACTED]</div> <div data-bbox="418 378 467 420">[REDACTED]</div> <div data-bbox="418 449 1425 529">[REDACTED]</div> <div data-bbox="418 558 467 600">[REDACTED]</div> <div data-bbox="418 630 1432 709">[REDACTED]</div> <div data-bbox="418 739 467 781">[REDACTED]</div> <div data-bbox="418 810 906 890">[REDACTED]</div> <div data-bbox="418 919 581 961">[REDACTED]</div> <div data-bbox="418 991 1091 1071">[REDACTED]</div> <div data-bbox="418 1100 467 1142">[REDACTED]</div> <div data-bbox="418 1171 1318 1507">[REDACTED]</div> <div data-bbox="418 1579 756 1621">[REDACTED]</div> <div data-bbox="418 1621 911 1663">FORTINET-NPS-SC 000064-000065</div> <div data-bbox="418 1692 553 1734">[862:867]</div> <div data-bbox="418 1764 1351 1843">[REDACTED]</div>
--	--

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000015-000034

[4:5]

[REDACTED]

[24:25]

[REDACTED]

[843:864]

[REDACTED]

[REDACTED]

[REDACTED]

(Tab 22)

FORT-NPS-SC0000336 (POP3 proxy code moving data across connections)

(Tab 5)

FORT-NPS-SC0000619-620 (NNTP proxy code moving data across connections)

(Tab 15)

FORT-NPS-SC0000404-405 (SMTP proxy code moving data across connections)

(Tab 24)

FORT-NPS-SC0000296 (IMAP proxy code moving data across connections)

(Tab 27)

FORT-NPS-SC0000249 (FTP proxy code moving data across connections)

(Tab 29)

FORT-NPS-SC0000210-211 (general code, across all proxies, for reading from/writing to connections to client and server)

(Tab 31)

FORT-NPS-SC0000199-201 (code for passing sockets from the acceptor to a proxy)
Same also on Tab 47, FORT-NPS-SC0000856-858

(Tab 44)

FORT-NPS-SC0000867-868 (code for returning content scanning results to the requesting proxy)

(Tab 45)

FORT-NPS-SC0000974 proxy acceptor / proxy worker initialization code

(Tab 48) Worker code

(Tab 52) Acceptor code.

To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the original transparent application layer proxies used with the accused products or the transparent application layer proxies that utilize a transparent proxy that controls or instructs a scan unit to perform application layer filtering with the accused products is interchangeable or substitutable for this claim limitation / element; and that neither the original transparent application layer proxies or the subsequent transparent application layer proxies play a role which is substantially different.

For instance, the 2005 configuration of a transparent application layer proxy formed by a proxy routine that controls and instructs a scan unit routine, is readily understood as the equivalent of this claim limitation / element, it one were to assert that it does not literally satisfy this claim limitation / element. The 2005 configuration of a transparent application layer proxy provide substantially the same function, which is to establish separate communication sessions with a source and a destination and to transparently transfer data between the source and destination through the application layer proxy, without requiring the sender to explicitly identify the firewall, in substantially the same way, which is by receiving packets that have the hardware address (MAC address) of the gateway, establishing a communication session with the source through the proxy process if there is an application layer proxy assigned to the destination port number, and subsequently

	<p>establishing a communication session with the destination through the proxy process, to achieve substantially the same result, which is to provide a firewall that utilizes a transparent application layer proxy process.</p> <p>Similarly, the 2010 configuration of a transparent application layer proxy formed by and acceptor routine and a proxy routine that controls and instructs a scan unit routine, can also be understood to be the equivalent of this claim limitation / element, it one were to assert that it does not literally satisfy this claim limitation / element. The 2010 configuration of a transparent application layer proxy provide substantially the same function, which is to establish separate communication sessions with a source and a destination and to transparently transfer data between the source and destination through the application layer proxy, without requiring the sender to explicitly identify the firewall, in substantially the same way, which is by receiving packets that have the hardware address (MAC address) of the gateway, establishing a communication session with the source through the proxy process if there is an application layer proxy assigned to the destination port number, and subsequently establishing a communication session with the destination through the proxy process, to achieve substantially the same result, which is to provide a firewall that utilizes a transparent application layer proxy process.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>57. Apparatus for providing a secure gateway for data changes between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process is further adapted to perform a data sensitivity check is on the data associated with each packet while transparently passing the data portion of the each packet.</p>	<p>FortiGate security devices implement UTM components which perform data sensitivity checking while transferring data. The below is an exemplary data sensitivity check and applies to all data sensitivity checks done in Fortinet source code.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Chapter 6</i></p> <div data-bbox="418 1409 878 1451" style="background-color: black; height: 20px; width: 283px;"></div> <p>FORTINET-NPS-SC 000125-000126</p> <p>[5:8]</p> <div data-bbox="418 1591 1170 1745" style="background-color: black; height: 73px; width: 463px;"></div>

[REDACTED]
FORTINET-NPS-SC 000127

[8:11]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000128

[11:35]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000129-000130

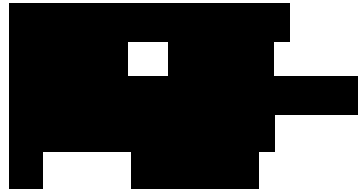
[11]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000131

[8:13]

[REDACTED]



[REDACTED]
FORTINET-NPS-SC 000044-000045

[10:18]



(Tab 1)

FORT-NPS-SC0000604 (queue a request for AV/DLP scanning in NNTP)

FORT-NPS-SC0000602 (receive a response from AV/DLP scanning in NNTP)

(Tab 2)

FORT-NPS-SC0000567 (queue a request for AV checking with the AV engine)

FORT-NPS-SC0000568-569 (receive an AV scan response from the AV engine)

(Tab 3)

FORT-NPS-SC0000645 (perform antispam checking of email)

(Tab 6)

FORT-NPS-SC0000708-710 (perform antivirus scanning on a file)

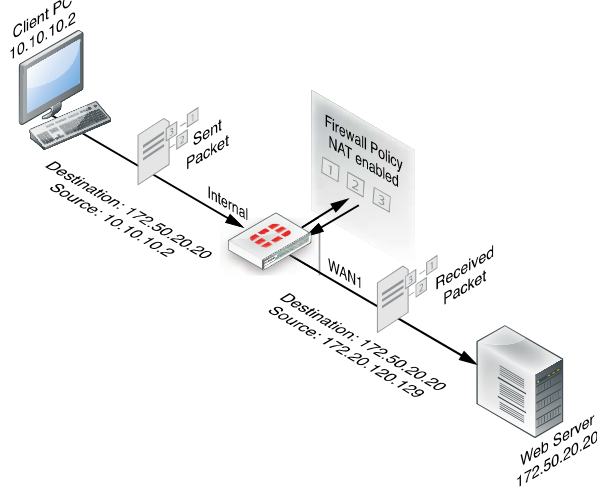
(Tab 11)

FORT-NPS-SC0000681-689 (perform DLP scanning on a file)
 FORT-NPS-SC0000684 (scan the body of a file/message for content)
 FORT-NPS-SC0000690 (DLP checking for HTTP)
 FORT-NPS-SC0000691 (DLP checking for Email)
 FORT-NPS-SC0000692 (DLP checking for FTP)
 FORT-NPS-SC0000693 (DLP checking for NNTP)
 FORT-NPS-SC0000694 (DLP checking for IM)
 (Tab 17)
 FORT-NPS-SC0000479 (scanning HTTP data at http proxy)

 (Tab 19)
 FORT-NPS-SC0000539 (perform URL filtering)

 (Tab 20)
 FORT-NPS-SC0000588 (scan for Slapper worm)

 (Tab 21)
 FORT-NPS-SC0000383 (act upon various results of scanning email messages)
 (Tab 23)
 FORT-NPS-SC0000319 (scanning of POP3 email messages)
 (Tab 25)
 FORT-NPS-SC0000278-279 (scanning of IMAP email messages)
 (Tab 28)
 FORT-NPS-SC0000214 (scanning of FTP transferred files)

	<p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the differences are interchangeable or substitutable for this claim limitation / element; and that the differences do not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>29. A computer system for providing a secure gateway between a private network and a potentially hostile network, comprising:</p>	<p>The purpose of firewalls is to act as secure gateways between a private ("protected") and a potentially hostile network, such as the Internet. The accused products, manufactured by Fortinet, act as firewalls, as is described in Fortinet's documentation (Handbook v3, page 183), website and source code.</p> <div data-bbox="430 955 1206 982" data-label="Caption"> <p>Figure 6: Sender's IP internal address translated to the FortiGate unit's external address</p> </div>  <p>(v2 FortiGate Fundamentals, p. 185)</p> <p>A. So, assuming that the FortiGate device is configured properly to do some sort of filtering, the client -- client side person, that computer would open their browser and type in a website. This will initiate a communication, a TCP connection, to go to the -- to the server. The FortiGate will be sitting in the middle.</p>

	<p><i>Crawford 30(b)(6) Dep. Trans. p. 99, lns. 6-11</i></p> <p>[REDACTED]</p> <p>FORTINET-NPS-SC 000066-000074</p> <p>[378:381]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>
<p>a) means for accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway;</p>	<p>Means Limitation: a) means for accepting</p> <p>Function: accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway;</p> <p>Structure: An operating system modified to handle communications packets differently than a standard Unix operating system kernel existing at the time of the invention and equivalents.</p> <p>Fig. 6 (64, 66); C9, L 40; C 9, L 65, C 10, L 9; C 4, L 48-51, L 59-64; C 5, L 40-44</p> <p>Linux was initially developed in 1991 by Linus Torvalds. Linus developed a new operating system kernel, using the same user-level tools (e.g., compiler, shell, other applications) as other Unix operating systems. Linux was released in September 1991. The first widely used Linux software distribution was released in 1993 under the name "Slackware". In June 1994, the Free Software Foundation (FSF), which sponsored the development of many of these user-level tools under the GNU Project, referred to Linux as "a free UNIX clone". Although the name "UNIX" is trademarked, it informally refers to a multitasking, multi-user computer operating system that follows conforms to several standards and has intellectually evolved from the first Unix system developed at AT&T Bell Labs in 1969. Linux users use substantially the same tools and utilities as Unix users; Linux system administrators manage device running Linux in substantially the same way as devices that run Unix; programmers develop code for Linux in substantially the same way as they do in Unix and in most situations programs developed for Linux can be easily ported to Linux and programs developed for Unix can be easily ported to Unix.</p>

The packet flow description in the Fortinet FortiOS handbook indicates that packets flow from either side of the gateway. These packets are accepted as long as they are encapsulated with the MAC address of the gateway. Packets traversing the FortiGate device addressed to the IP address of a host on a hostile network are encapsulated with the MAC address of the FortiGate device.

Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, Pp 184, 185

The Handbook v3, pages 707-708, describes, as an example, how a FortiGate device handles a packet transmitted from a web client to a web server and vice versa. Figure 69 on page 709 depicts graphically this process, which includes intercepting the packet, inspecting it through a variety of means, including a Proxy Inspection Engine that applies Antivirus and Web Filtering, and forwarding it if accepted by policy. Furthermore, the Handbook v3, pages 735-737, describes an example of a TCP connection between a client and server, to which various security policies are applied, showing how the packets are intercepted on either side and processed by FortiOS.

Q. Is there any address information contained in packets that are received by FortiGate device?

A. Yes.

Q. What kind of information?

A. There's a MAC address, IP address.

Crawford 30(b)(6) Dep. Trans. p. 126, lns. 7-11

[REDACTED]
FORTINET-NPS-SC 000066-000074

[378:381]

[REDACTED]
[REDACTED]

[REDACTED]

(Tab 38)

	<p>FORT-NPS-SC0000023-27 (code that sets the MAC address of an Ethernet interface, for two different types of Ethernet interfaces --- 100Mbps and 1000Mbps)</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that a gateway with a kernel that accepts a data packet with the MAC address of the accused product is interchangeable or substitutable for this claim limitation / element; and this kernel that accepts a data packet with the MAC address of the accused product does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>b) means for determining whether there is a process bound to a destination port number of an accepted communications packet;</p>	<p>Means Limitation: b) means for determining</p> <p>Function: determining whether there is a process bound to a destination port number of an accepted communications packet;</p> <p>Structure: An operating system modified to handle communications packets differently than a standard Unix operating system kernel existing at the time of the invention and equivalents.</p> <p>Fig. 6 (70); C 10, L 4-9; C 4, L 26-29;</p> <p>Linux was initially developed in 1991 by Linus Torvalds. Linus developed a new operating system kernel, using the same user-level tools (e.g., compiler, shell, other applications) as other Unix operating systems. Linux was released in September 1991. The first widely used Linux software distribution was released in 1993 under the name "Slackware". In June 1994, the Free Software Foundation (FSF), which sponsored the development of many of these user-level tools under the GNU Project, referred to Linux as "a free UNIX clone". Although the name "UNIX" is trademarked, it informally refers to a multitasking, multi-user computer operating system that follows conforms to several standards and has intellectually evolved from the first Unix system developed at AT&T Bell Labs in 1969. Linux users use substantially the same tools and utilities as Unix users; Linux system administrators manage device running Linux in substantially the same way as devices that run Unix; programmers develop code for Linux in substantially the same way as they do in Unix and in most situations programs developed for Linux can be easily ported to Linux and programs developed for Unix can be easily ported to Unix.</p>

	<p>FortiOS determines whether there is a process bound or assigned to a destination port number of an accepted communications packet by matching the packet to a policy: <i>“When a firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.”</i> (FortiOS Handbook v2, pages 191, 196-197, and 231.)</p> <p>These policies determine, among other things, whether a proxy, as stated in the Handbook v3, pages 705-706, will process a packet:</p> <p><i>“The policy look up is where the FortiGate unit reviews the list of security policies which govern the flow of network traffic, from the first entry to the last, to find a match for the source and destination IP addresses and port numbers. The decision to accept or deny a packet, after being verified as a valid request within the stateful inspection, occurs here. A denied packet is discarded. An accepted packet will have further actions taken. If IPS is enabled, the packet will go to Flow-based inspection engine, otherwise it will go to the Proxy-based inspection engine. If no other UTM options are enabled, then the session was only subject to stateful inspection. If the action is accept, the packet will go to Source NAT to be ready to leave the FortiGate unit.”</i></p> <p>The FortiGate device uses proxy processes to perform some of its security functionality. The Handbook v3, page 707, states:</p> <p><i>“The proxy inspection engine is responsible for carrying out antivirus protection, email filtering (antispam), web filtering and data leak prevention. The proxy engine will process multiple packets to generate content before it is able to make a decision for a specific packet.”</i></p> <p>“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).</p> <p>“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-NPS 017058-59; FORT-NPS 017008).</p> <p>“When the firewall receives a connection packet, it analyzes the packet’s source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).</p>
--	---

“If the initial packet matches the firewall policy, the FortiGate unit performs the configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if that initial TCP connection matches any of our policies.

Q. Okay. And if it does?

A. If it does match, then it will determine whether it's to pass that through or whether it's going to -- it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

These proxies are implemented as application-level (“user-level”) processes. This can be seen in the FortiOS source code:

[REDACTED]

FORTINET-NPS-SC 000035-000036

[803:804]

[REDACTED]

[808:856]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000043

[3:14]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000039-000043

[9:16]

[REDACTED]

[124:126]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000037-000038

[4:5]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000066-000074

[58:67]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000110-000114

[1711:1716]

[REDACTED]

	<div style="background-color: black; width: 100%; height: 20px; margin-bottom: 10px;"></div> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the policies stored in the configuration file and written to the OS kernel of the accused products is interchangeable or substitutable for this claim limitation / element; and the manner in which accused products employ policies does not play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
<p>c) means for establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;</p>	<p>Means Limitation: c) means for establishing</p> <p>Function: establishing a first communications session with a source address/source port of the accepted communications packet.</p> <p>Structure: An operating system modified to handle communications packets differently than a standard Unix operating system kernel existing at the time of the invention, and a process, a generic process, a proxy process or a custom proxy process, and equivalents.</p> <p>Fig. 6 (76); C 10, L 14-19; Fig 4 (14, 16); C 4 L 29- 33; C 4 L 65; C 8, L 50-54</p> <p>Linux was initially developed in 1991 by Linus Torvalds. Linus developed a new operating system kernel, using the same user-level tools (e.g., compiler, shell, other applications) as other Unix operating systems. Linux was released in September 1991. The first widely used Linux software distribution was released in 1993 under the name "Slackware". In June 1994, the Free Software Foundation (FSF), which sponsored the development of many of these user-level tools under the GNU Project, referred to Linux as "a free UNIX clone". Although the name "UNIX" is trademarked, it informally refers to a multitasking, multi-user computer operating system that follows conforms to several standards and has intellectually evolved from the first Unix system developed at AT&T Bell Labs in 1969. Linux users use substantially the same tools and utilities as Unix users; Linux system administrators manage device running Linux in substantially the same way as devices that run Unix; programmers develop code for Linux in substantially the same way as they do in Unix and in most situations programs developed for Linux can be easily ported to Linux and programs developed for Unix can be easily ported to Unix.</p>

As noted above, the accused products examine a packet's source address, destination address and port number to determine if there is a policy and consequently an applicable transparent application layer proxy that is assigned to the port number.

If a policy match is made during the Packet Flow: Ingress processing, then a first communications session is transparently established between the source and the gateway (as indicated by creating an entry in the session table), otherwise the packet is dropped. (Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 193-194.) The creation of the first communication session between the source and the gateway, instead of the destination, would not be apparent to the initiator.

If the accused products determine that there is not a policy assigned to the destination port number identified in the packet, then the packet will be dropped.

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

“Firewall policies provide the instructions to the FortiGate unit as to what traffic is allowed through the device.” (FORT-NPS 017055).

“Firewall policies are instructions the Fortinet unit uses to decide connection acceptance and packet processing for traffic attempting to pass through.” (FORT-NPS 017058-59; FORT-NPS 017008).

“When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.” (FORT-NPS 017058-59; FORT-NPS 017008).

“If the initial packet matches the firewall policy, the FortiGate unit performs the configures Action and any other configured options on all packets in the session. Packet handling actions can be ACCEPT, DENY, IPSEC or SSL-VPN.” (FORT-NPS 017058-59).

“ACCEPT policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more UTM profiles to apply features such as virus scanning to packets in the session.” (FORT-NPS 017058-59).

“If no policy matches, the connection is dropped.” (FORT-NPS 017059).

Q. And explain for me what a policy is.

A. It's a -- it's a rule. It's a rule to allow traffic to pass from one interface through to the another interface of the product.

Q. And how or from where does FortiGate get policies?

A. Where does it get policies?

Q. Mm-hmm.

A. We have a policy table.

Q. And where in the product does that policy table reside?

A. We have -- the policy is recorded in our configuration and -- and is installed down into the kernel.

Crawford 30(b)(6) Dep. Trans. p. 51, lns. 3-16

Q. All right. And how is the policy used by the kernel?

A. It's used by the kernel to match against traffic.

Crawford 30(b)(6) Dep. Trans. p. 55, lns. 5-8

A. ...the kernel will go through the policies and see if that initial TCP connection matches any of our policies.

Q. Okay. And if it does?

A. If it does match, then it will determine whether it's to pass that through or whether it's going to -- it needs further processing.

Crawford 30(b)(6) Dep. Trans. p. 99, lns. 13-18

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

This is also supported by the source code, which clearly indicates that FortiOS manages the two connections separately.

[REDACTED]

FORTINET-NPS-SC 000066-000074

[4:9]

[REDACTED]

[196:200]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000119-000124

[37:41]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000115-000116

[36:69]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000117-000118

[22:51]

[REDACTED]

relevant:

FORTINET-NPS-SC 000109

(Tab 4)

FORT-NPS-SC0000641 (receive a connection at the IMD proxy)

(Tab 5)

FORT-NPS-SC0000622 (receive a client connection, for the NNTP proxy)

(Tab 15)

FORT-NPS-SC0000409 (receive a client connection, for the SMTP proxy)

(Tab 22)

FORT-NPS-SC0000338 (receive a client connection, for the POP3 proxy)

(Tab 24)

FORT-NPS-SC0000298-300 (receive a client connection, IMAP proxy)

(Tab 27)

FORT-NPS-SC0000252-253 (receive a client connection, FTP proxy)

FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data)

To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the transparent proxies or worker proxies of the accused products is interchangeable or substitutable for this claim limitation / element; and that these transparent proxies or worker proxies do not play a role which is substantially different.

I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further

	discovery, deposition testimony, and any other pertinent court ruling.
d) means for transparently establishing, without intervention from the source, a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and	<p>Means Limitation: d) means for transparently establishing</p> <p>Function: transparently establishing, without intervention from the source, a second communications session with a destination address/destination port of the accepted communications packet.</p> <p>Structure: A process, a proxy process, a generic process, generic proxy process or a custom proxy process, and equivalents.</p> <p>Fig. 4 (14, 46) C 4, L 33-36; Fig. 7b (104), C 4, L 33- 36; C 5, L2; C 8, L 58; C 11, L 66 – C 12, L 7</p> <p>Linux was initially developed in 1991 by Linus Torvalds. Linus developed a new operating system kernel, using the same user-level tools (e.g., compiler, shell, other applications) as other Unix operating systems. Linux was released in September 1991. The first widely used Linux software distribution was released in 1993 under the name "Slackware". In June 1994, the Free Software Foundation (FSF), which sponsored the development of many of these user-level tools under the GNU Project, referred to Linux as "a free UNIX clone". Although the name "UNIX" is trademarked, it informally refers to a multitasking, multi-user computer operating system that follows conforms to several standards and has intellectually evolved from the first Unix system developed at AT&T Bell Labs in 1969. Linux users use substantially the same tools and utilities as Unix users; Linux system administrators manage device running Linux in substantially the same way as devices that run Unix; programmers develop code for Linux in substantially the same way as they do in Unix and in most situations programs developed for Linux can be easily ported to Linux and programs developed for Unix can be easily ported to Unix.</p>

Depending on the action(s) determined by policy and the first communications session, the session table is transparently updated to indicate a second communications session with a destination address/destination port associated with the accepted communications packet. The Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, pages 186-187 and 193 state:

“Part of the stateful inspection engine, session tracking maintains session tables that maintain information about sessions that the stateful inspection module uses for maintaining sessions, NAT, and other session related functions.”

The creation of the second communication session between the destination and the gateway, instead of between the source and the destination, would not be apparent to the initiator.

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

A. ...So now the connection is with that proxy worker. And then the proxy worker will make the final connection out to the server, and then the communications between the client and the -- and the server are observed.

Crawford 30(b)(6) Dep. Trans. p. 100, lns. 1-6

The FortiOS source code also shows that :

[REDACTED]

FORTINET-NPS-SC 000066-000074

[196:200]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000058-000063

[1158:1422]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[43:48]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000110-000114

[59:63]

[REDACTED]

[1711:1719]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000140-000145

[1456:1476]



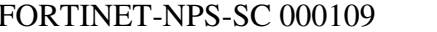
[REDACTED]

[REDACTED]

[REDACTED]

[3190:3194]

[REDACTED]

	<p>   relevant:  FORTINET-NPS-SC 000109 (Tab 5) FORT-NPS-SC0000611-613 (connect to the server, for the NNTP proxy) (Tab 15) FORT-NPS-SC0000396 (SMTP proxy connects to the server) (Tab 22) FORT-NPS-SC0000327-330 (POP3 proxy connects to the server) (Tab 24) FORT-NPS-SC0000287-290 (IMAP proxy connects to the server) (Tab 27) FORT-NPS-SC0000238-241 (connect to the server, for FTP proxy) FORT-NPS-SC0000241-242 (accept a connection from the client and connect to the FTP server, for transferring the actual data) </p> <p> To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the transparent proxies or worker proxies of the accused products is interchangeable or substitutable for this claim limitation / element; and that these transparent proxies or worker proxies do not play a role which is substantially different. </p> <p> I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling. </p>
e) means for transparently moving	Means Limitation: e) means for transparently moving

<p>data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.</p>	<p>Function: transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions.</p> <p>Structure: A process, a proxy process, a generic process, generic proxy process or a custom proxy process, and equivalents.</p> <p>Fig. 4 (14); C 4, L 38-43; C 5, L 4-8; Fig. 7b (106); C 12, L 8-15</p> <p>Linux was initially developed in 1991 by Linus Torvalds. Linus developed a new operating system kernel, using the same user-level tools (e.g., compiler, shell, other applications) as other Unix operating systems. Linux was released in September 1991. The first widely used Linux software distribution was released in 1993 under the name "Slackware". In June 1994, the Free Software Foundation (FSF), which sponsored the development of many of these user-level tools under the GNU Project, referred to Linux as "a free UNIX clone". Although the name "UNIX" is trademarked, it informally refers to a multitasking, multi-user computer operating system that follows conforms to several standards and has intellectually evolved from the first Unix system developed at AT&T Bell Labs in 1969. Linux users use substantially the same tools and utilities as Unix users; Linux system administrators manage device running Linux in substantially the same way as devices that run Unix; programmers develop code for Linux in substantially the same way as they do in Unix and in most situations programs developed for Linux can be easily ported to Linux and programs developed for Unix can be easily ported to Unix.</p> <p>Once the first and second sessions (between the firewall and source, and between firewall and destination) are established, the Stateful Inspection feature provides for all subsequent packets in the same application layer session to be moved transparently between the sessions. The transfer of data between each communication session through the proxy process would not be apparent to the initiator.</p> <p><i>Fortinet FortiOS Handbook v2 for FortiOS 4.0 MR2, P. 189, Chapter 6.</i></p>
--	--

Proxies

Application Proxies

Each protocol that can be inspected has a dedicated transparent proxy in the FortiOS architecture. This proxy sits between the client and the server intercepting all connections (requests and responses).

Tasks performed by the protocol proxies include:

- Making decisions

The proxy, in cooperation with the inspection daemons (antivirus, antispam or webfiltering) is responsible for making the decision to buffer, pass or block data passing through the FortiGate based on the policies in place.

(Course 301-v4.0 Secured Network Deployment and Virtual Private Networks, p. 281)

The Scanner Proxy

The firewall uses a transparent proxy to handle incoming email protocols POP3 (Post Office Protocol) and IMAP4 (Internet Message Access Protocol) and outgoing email using SMTP (Simple Mail Transfer Protocol). Http file uploads and downloads will be handled via a second proxy program. The advantage to using a transparent proxy is that the client and server programs need no special configuration to communicate; the connection is diverted to the proxy, which sets up connections to the client and server. Once the connections are setup the traffic on the connection is parsed for key commands, based on the protocol being used by the connection, and email or file upload/downloads are intercepted. Most intercepted upload/downloads will use the MIME (Multipurpose Internet Mail Extensions) format. The MIME file will be parsed, looking for target attachments such as executable files or scripts (visual basic, MSWORD documents with macros etc.). If in High security mode once a target attachment is found the attachment will be replaced immediately. If in Medium security mode the attachment will be scanned by the virus engine and if it is clean will be reattached to the appropriate email or http upload/download message. If a virus is found in the attachment the attachment will

be replaced with a message and the attachment is either quarantined for download by and administrator or destroyed.

FORT-NPS 169248-169249

In the following example, the client makes a request and expects to receive data in response. This is for illustration purposes only; in some protocols the roles are reversed: that is, the server receives the bulk of the data in the transaction.

From the point view of the client, this is what happens:

1. client connects to server and makes request
2. server sends back response.

In fact, the transparent proxy between the client and the server intercepts all connections, requests and responses. The proxy buffers and scans the server's response before flushing it to the client. While buffering and flushing the naive proxy implementation sends no information to the client and server, respectively.

FORT-NPS 165878

traffic such as incoming traffic through VIP or Port Forwarding; redirect table
 [REDACTED] is for those traffic that need to go through our
 transparent proxies, such as anti-virus engine, for further processing;

FORT-NPS 164710

A. Okay. The transparent proxy, the user does not need to configure their browser, so they'll just use their browser, their computer goes on the network with the -- and it will make a request to try to visit the website, and FortiGate will be in the middle and can intercept that communication. And the content of the communication can be buffered and given to another program to apply the antivirus filter on it. And, again, if everything is okay, then it can either let the trafficking through or block it or perform other actions on it.

Crawford 30(b)(6) Dep. Trans. p. 92 lns. 7-17

This can be seen in the FortiOS source code:

[REDACTED]

FORTINET-NPS-SC 000066-000074

[201:204]

[REDACTED]

[269:275]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000119-000124

[50:54]

[REDACTED]

[250:258]

[REDACTED]

[REDACTED]
FORTINET-NPS-SC 000075-000077

[32:96]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000140-000145

[3997:4013]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000064-000065

[862:867]

[REDACTED]

[REDACTED]

[REDACTED]

FORTINET-NPS-SC 000015-000034

[4:5]

[REDACTED]

[24:25]

[REDACTED]

[843:864]

[REDACTED]

[REDACTED]

[REDACTED]

(Tab 22)

FORT-NPS-SC0000336 (POP3 proxy code moving data across connections)

(Tab 5)

FORT-NPS-SC0000619-620 (NNTP proxy code moving data across connections)

(Tab 15)

FORT-NPS-SC0000404-405 (SMTP proxy code moving data across connections)

(Tab 24)

FORT-NPS-SC0000296 (IMAP proxy code moving data across connections)

(Tab 27)

FORT-NPS-SC0000249 (FTP proxy code moving data across connections)

(Tab 29)

FORT-NPS-SC0000210-211 (general code, across all proxies, for reading from/writing to connections to client and server)

(Tab 31)

FORT-NPS-SC0000199-201 (code for passing sockets from the acceptor to a proxy)
Same also on Tab 47, FORT-NPS-SC0000856-858

(Tab 44)

FORT-NPS-SC0000867-868 (code for returning content scanning results to the requesting proxy)

	<p>(Tab 45) FORT-NPS-SC0000974 proxy acceptor / proxy worker initialization code</p> <p>(Tab 48) Worker code</p> <p>(Tab 52) Acceptor code.</p> <p>To the extent that Fortinet suggests that the accused products do not literally satisfy this claim limitation / element, then the accused products satisfy this claim limitation / element under the doctrine of equivalents. As shown by at least the evidence cited above, the differences, if any, between the accused products and this claim limitation / element are insubstantial at most. One of ordinary skill in the art, to which the '601 patent pertains, would understand that the original transparent application layer proxies used with the accused products or the transparent application layer proxies that utilize a transparent proxy that controls or instructs a scan unit to perform application layer filtering with the accused products is interchangeable or substitutable for this claim limitation / element; and that neither the original transparent application layer proxies or the subsequent transparent application layer proxies play a role which is substantially different.</p> <p>I reserve the right to further supplement my opinions as to equivalence after reviewing the response of Fortinet's expert(s), the production of any further discovery, deposition testimony, and any other pertinent court ruling.</p>
--	--